ARTICLE DE LA REVUE JURIDIQUE THÉMIS

On peut se procurer ce numéro de la Revue juridique Thémis à l'adresse suivante :
Les Éditions Thémis
Faculté de droit, Université de Montréal
C.P. 6128, Succ. Centre-Ville
Montréal, Québec
H3C 3J7

Téléphone : (514)343-6627
Télécopieur : (514)343-6779
Courriel : themis@droit.umontreal.ca

La sécurité des opérations bancaires par Internet*

Marc LACOURSIÈRE** et Édith VÉZINA***

Résumé

Les services bancaires en ligne offerts par les institutions financières canadiennes sont maintenant aussi complets que ceux disponibles en succursale. Ces développements technologiques ont favorisé de nombreux cas de fraudes, ce qui a eu pour conséquence de miner la confiance des consommateurs. La cryptographie à clé publique s'est imposée comme une tentative de solution à ce problème, et elle est maintenant encadrée par le législateur québécois dans la Loi concernant le cadre juridique des technologies de l'information. Les spécialistes affirment que l'efficacité de cette cryptographie tient à un critère fondamental, soit l'indépendance du tiers certificateur. À nos yeux, un second critère est tout aussi essentiel, soit

Abstract

Online banking services offered by Canadian financial institutions are now as complete as those traditionally available. These new technological developments have fostered several kinds of fraudulent scams, which have eroded consumer confidence. Public key cryptography is now a prominent solution to this issue, and it is now recognized by the Quebec legislator in the Act to Establish a Legal Framework for Information Technology. Specialists argue that the independence of the third party is a fundamental principal of the efficiency of cryptography. We argue that another criterion is as much important: a hierarchy of third parties, since it may help the integrity and the respect of the process by each intermediary. This

* Les auteurs désirent remercier la Fondation Claude Masse pour le financement de cet article. Sous réserve d'une indication contraire quant à la date d'accès, la consultation des sites Internet cités dans le présent article est à jour au 8 juin 2006.

** Avocat, professeur à la Faculté de droit de l'Université Laval, et membre du comité de direction du Centre d'études en droit économique de la Faculté de droit de l'Université Laval.

*** Notaire, doctorante à la Faculté de droit de l'Université Laval, chargée de cours à la Faculté de droit de l'Université de Sherbrooke, et membre du Centre d'études en droit économique de la Faculté de droit de l'Université Laval.

l'instauration d'une hiérarchie de tiers certificateurs, laquelle permet d'assurer l'intégrité et le respect du processus par chaque intermédiaire. Cette infrastructure hiérarchique est difficile à mettre en place, certes, mais elle se justifie par la nécessité de rehausser la sécurité des opérations bancaires par Internet afin d'assurer une meilleure protection des consommateurs.

may be difficult to put forward, but it is justified by the necessity to secure online banking services in order to better protect consumers.

Plan de l'article

Les institutions financières canadiennes offrent une panoplie de services bancaires dans leur vitrine Internet. Ce nouveau canal de distribution présente des avantages évidents pour les consommateurs – diminution des coûts, rapidité et flexibilité, notamment. Toutefois, de nombreux cas de fraudes ont révélé des problèmes de sécurité dans Internet, non seulement du point de vue technique, mais également du point de vue juridique, ce qui a eu pour conséquence de miner la confiance des consommateurs. Plusieurs tentatives ont été proposées pour contrer ce fléau, dont le développement de la cryptographie à clé publique, également appelée cryptographie asymétrique. Utilisée depuis des millénaires, la cryptographie a été adaptée récemment aux communications en ligne. La cryptographie à clé publique permet à deux intervenants de se transmettre des informations chiffrées par l'entremise d'une tierce personne – appelée tiers certificateur ou autorité de certification – qui certifie l'origine des données et la sécurité de celles-ci durant la transmission dans un environnement ouvert – c'est-à-dire par Internet. Cette nouvelle technologie est maintenant utilisée d'une manière généralisée et elle est également reconnue par le législateur québécois dans la *Loi concernant le cadre juridique des technologies de l'information*[1].

Bien que ces développements apparaissent sécurisants à première vue, il en va autrement en réalité. La sécurité des transactions en ligne ne pourra jamais être réalisée à cent pour cent, certes, mais il est possible de réduire les risques. Il est nécessaire qu'un tiers certificateur soit indépendant, c'est-à-dire qu'il ne soit sous le contrôle ni du transmetteur, ni du récepteur de l'information transmise. Afin de renforcer la sécurité, une hiérarchie de tiers certificateurs permet d'assurer l'intégrité et le respect du processus par chaque intermédiaire. Brièvement, ce concept signifie que le certificateur de niveau de base – en contact direct avec les cocontractants – est supervisé par un autre certificateur – appelé autorité de certification (tiers certificateur) de niveau supérieur –, et ainsi de suite. Pour le moment, une telle infrastructure hiérarchique est difficile à mettre en place, non seulement pour des raisons techniques, mais également pour des motifs d'ordre juridique. Cette constatation étant établie, il convient de formuler les trois hypothèses suivantes : 1° les autorités de certification opérées par les banques n'offrent

---

1 L.R.Q., c. C-1.1.

pas l'indépendance requise, ce qui cause une lacune majeure dans la sécurité des opérations bancaires et affecte le niveau de confiance des consommateurs ; 2° une infrastructure hiérarchique d'autorités de certification doit être mise en place dans le secteur bancaire canadien afin de sécuriser les opérations bancaires ; bien qu'elle réglemente les signatures électroniques et la certification, la législation canadienne demeure inadéquate pour réglementer une telle infrastructure ; 3° il est nécessaire que les provinces canadiennes tendent vers une certaine forme d'harmonisation en matière de sécurité des opérations bancaires par Internet pour assurer une meilleure protection des consommateurs.

La première partie de ce texte présente un état des lieux de la certification. Nous présentons d'abord les conséquences de la sécurité pour analyser ensuite les principales tentatives de solution d'ordre juridique et technique. La seconde partie est destinée à l'étude de la supervision des certificateurs. Nous examinons les divers modes de supervision pour traiter par la suite de la responsabilité de la banque dans ce processus.

I. L'état des lieux de la sécurité des transactions bancaires

La sécurité des opérations en ligne constitue certainement la pierre angulaire du commerce électronique, car ses lacunes expliquent principalement les réticences des usagers envers celles-ci. Cette première partie présente les tenants et les aboutissants des notions de sécurité. D'abord, nous examinons les notions entourant la sécurité, soit la raison d'être de la sécurité et, le corollaire, les fondements de la certification (A). Ensuite, nous analysons les diverses tentatives de solution. S'agissant des solutions d'ordre juridique, nous constatons leur évolution depuis plusieurs années de l'état d'autorégulation vers une régulation étatique. Parallèlement, les moyens techniques se sont également perfectionnés (B). Il va sans dire que ces éléments sont interreliés et s'influencent mutuellement.

A. La sécurité des transactions bancaires

Puisqu'il serait utopique de prétendre offrir un niveau de sécurité parfaitement étanche, il importe de constater quelles sont les

lacunes des sites bancaires en ligne. Les conséquences de ces lacunes ont trait principalement à la vulnérabilité de la sécurité, ce qui est susceptible d'engendrer une certaine réticence des consommateurs et des usagers envers les transactions bancaires en ligne (1). Les auteurs sont très majoritairement d'avis que la certification permet, non pas de résoudre, mais de tempérer les lacunes qui découlent de la sécurité. Nous présentons dans la sous-section suivante les fondements de la certification (2).

1. La raison d'être de la sécurité

Historiquement, les banques ont été confinées à l'exécution des ordres de paiement, d'une part, et à la réception des dépôts ainsi qu'à l'octroi de prêts, d'autre part. Le rôle des banques en tant qu'intermédiaires dans le système des paiements et dans la gestion du crédit connaît présentement des transformations majeures en raison de la diversité croissante des services offerts et des développements technologiques qui bouleversent les habitudes des consommateurs, tant en ce qui a trait aux modes de paiement, au crédit à la consommation, qu'aux autres services bancaires. Au Canada, notamment, les banques à charte canadiennes et les quasi-banques – institutions financières autres que les banques à charte – offrent maintenant à leur clientèle la plupart de leurs opérations bancaires courantes par le truchement des communications électroniques : ouverture de compte, virements de fonds entre comptes de la même succursale ou entre succursales de la même banque, paiement de factures, remboursement d'une marge de crédit et possibilité d'effectuer des demandes de prêt. Ces services sont complémentaires aux services offerts traditionnellement. De nouveaux intermédiaires commerciaux offrent également aux consommateurs des services bancaires en ligne, analogues à ceux des banques et quasi-banques traditionnelles. Quelques-uns de ces services sont avant-gardistes : services de certification des cartes de crédit transmises par Internet, chèques électroniques et micropaiements, aussi connus sous le nom de monnaie digitale ou virtuelle.

Cette nouvelle génération de services bancaires apporte des avantages indéniables aux consommateurs, tels une diminution relative des coûts, un accès plus rapide, des horaires plus flexibles et des marchés plus vastes. Du point de vue de la rationalité des échanges économiques, le développement du commerce en ligne traduit donc une évolution positive. Les statistiques révèlent que les

consommateurs canadiens deviennent de moins en moins méfiants vis-à-vis de l'utilisation d'Internet pour effectuer leurs transactions bancaires. À titre d'exemple, selon une étude de ACNielsen Canada, environ 75 % des Canadiens transigent maintenant par le réseau Internet, et environ 59 % effectuent régulièrement des opérations de services financiers en ligne, par rapport à 54 % en 2003 et à 50 % en 2002[2]. Or, il faut être prudent en analysant ces chiffres, puisqu'une étude de l'Association des banquiers canadiens (ci-après citée « ABC ») de 2003 indiquait que seize pour cent des consommateurs utilisaient principalement Internet pour effectuer leurs transactions bancaires et qu'environ les deux tiers demeurent réticents à utiliser le commerce électronique[3]. D'ailleurs, les activités commerciales via Internet demeurent l'apanage presque exclusif du milieu des affaires – 80 % du marché –, malgré les tentatives des entreprises pour attirer les consommateurs.

Les études de l'ABC et de la Clearing House Interbank Payments System (ci-après citée « CHIPS ») suggèrent que certains obstacles juridiques peuvent exister au Canada et freiner le développement des transactions bancaires en ligne[4]. La principale barrière juridique qui nuit au développement des pratiques bancaires dans Internet prend sa source dans la vulnérabilité de la sécurité de ces transactions en ligne – problème intrinsèque à Internet. Sous l'angle juridique, cette lacune se traduit par une ambiguïté quant à la réglementation des intervenants – notamment les tiers certificateurs – ainsi que par une diversité des règles à travers le Canada. En fait, depuis sa naissance, Internet souffre d'une incertitude technique et juridique, comme le démontrent les nombreux exemples de fraudes. Cette situation engendre une timidité de la part des consommateurs, qui craignent l'interception d'une information par un pirate de l'informatique et, le cas échéant, la difficulté, sinon l'impossibilité, pour une victime d'obtenir réparation légale. À cet égard, il con-

---

2 ACNIELSEN CANADA, « Three out of Five Internet Users Take Advantage of Online Financial Services », 5 avril 2006, en ligne : [http://www.acnielsen.ca/news/20060405.shtml] ; Michel MUNGER, « La banque en ligne gagne en popularité », *LaPresseAffaires.com* (5 avril 2006), en ligne : [http://www.LaPresseAffaires.com].

3 ABC, « Technologie et services bancaires : sondage sur les attitudes des clients », 2003, en ligne : [http://www.cba.ca/fr/viewdocument.asp?fl=3&sl=142&tl=&docid=408&pg=1].

4 *Id.* ; CHIPS, *The Remaining Barriers to ePayments and Straight-through Processing*, octobre 2001-mars 2002, p. 6, en ligne : [http://www.chips.org/infofiles/CHIPS_Remaining_Barriers.pdf].

vient de rappeler l'importance des fraudes touchant les paiements en ligne : alors que les transactions commerciales dans Internet ne représentent que deux pour cent des transactions totales, elles génèrent près de cinquante pour cent des réclamations auprès des émetteurs de cartes de paiement[5].

2. Les fondements de la certification

Le *Petit Robert* définit la certification comme suit : « Assurance donnée par écrit. Certification de signatures, de chèques »[6]. Au verbe « certifier », ce dictionnaire mentionne : « Assurer qu'une chose est vraie. [...] Garantir par un acte »[7]. En droit cambiaire, la certification d'un chèque est un usage bancaire centenaire qui consiste pour le bénéficiaire à requérir le visa de la banque tirée lorsqu'il exprime un doute sur la solvabilité du tireur[8]. Comme le rappelle à juste titre M^e^ Bernard Brun :

> *La certification en matière commerciale est un concept relativement nouveau dont la signification peut varier selon le domaine dans lequel on se trouve. Ce mot, proche parent de « certificat », existe depuis longtemps, mais s'est acquis une nouvelle renommée avec l'ouverture des marchés. Tout comme son cousin, il provient du terme latin* « certus », *qui signifie : décidé, résolu, arrêté, fixé, déterminé, précis, convenu, certain, sûr, clair, manifeste, fidèle.*[9]

Concept ancien[10], la certification a repris du service sous Internet. Son rôle est de sécuriser une transaction qui se déroule en ligne. Lors d'une opération bancaire, un intermédiaire fait le pont entre

---

5 Jean ALLIX, « La politique communautaire dans le domaine des moyens de paiement : l'espace unique de paiement », (2000) *Revue européenne de droit de la consommation* 337, 357.

6 Paul ROBERT, Josette REY-DEBOVE et Alain REY, *Le nouveau Petit Robert – Dictionnaire alphabétique et analogique de la langue française*, Paris, Dictionnaire le Robert, 2000, p. 374.

7 *Id.*

8 Nicole L'HEUREUX, Édith FORTIN et Marc LACOURSIÈRE, *Droit bancaire*, 4^e^ éd., Cowansville, Éditions Yvon Blais, 2004, n^o^ 2.120, p. 572.

9 Bernard BRUN, « Nature et impacts juridiques de la certification dans le commerce électronique sur Internet », mars 2000, (2001) 7(1) *Lex Electronica* 3, en ligne : [http://www.lex-electronica.org/articles/v7-1/Brun.pdf].

10 La science de la cryptographie est très ancienne. Les premières méthodes de chiffrements remontent à l'antiquité. Cette technique fut principalement utilisée à des fins militaires et s'est perfectionnée au fil des siècles. La version moderne

un client et une banque. Dans les faits, cet intermédiaire prend la forme d'un tiers indépendant. Il peut agir en tant que réseau de communication afin de permettre aux usagers de se brancher sur la grande toile que représente Internet. Son rôle est donc passif. Il peut également intervenir en tant qu'autorité de certification. Son rôle est alors actif : transmission de documents, délivrance de certificats, vérification de signatures et gestion des certificats[11]. La signature électronique est donc la pierre angulaire du commerce électronique. Cette signature peut être sécurisée ou non, selon qu'elle est transmise ou non par une méthode de chiffrement. Le cas échéant, elle peut être chiffrée par deux méthodes principales, soit par un procédé appelé biométrie[12], soit par la cryptographie à clé publique[13].

---

du premier système de cryptographie à clé publique – ou cryptographie asymétrique – a été mise au point en 1976. Pour une analyse historique de ce système, voir notamment : Carl M. ELLISON, « Certification Infrastructure Needs for Electronic Commerce and Personal Use », (1998) 2 (2) *Elec. Banking L. & Com. Rep.* 9 ; Lonnie ELDRIDGE, « Internet Commerce and the Meltdown of Certification Authorities : Is the Washington State a Good Model ? », (1998) 45 *UCLA L. Rev.* 1805, 1818 et 1819 ; WIKIPEDIA, « L'histoire de la cryptographie », *Wikipedia – L'encyclopédie libre*, 2006, en ligne : [http://fr.wikipedia.org/wiki/Histoire_de_la_cryptographie].

11 Henry H. PERRITT, Jr., *Law and the Information Superhighway: Privacy, Access, Intellectual Property, Commerce, Liability*, New York, J. Wiley & Sons, 1996, p. 396 et 397.

12 La biométrie consiste à identifier des personnes en se basant sur des caractéristiques personnelles individuelles. À ce sujet, voir généralement : Richard HOPKINS, « An Introduction to Biometrics and Large Scale Civilian Identification », (1999) 13 *Int'l Rev. of L. Computers & Tech.* 337 ; Robert R. JUENEMAN et R.J. ROBERTSON, Jr., « Biometrics and Digital Signature in Electronic Commerce », (1998) 38 *Jurimetrics J.* 427. Aux fins de ce texte, nous ne traiterons pas du procédé biométrique.

13 En pratique, le fonctionnement de la cryptographie à clé publique s'apparente à ceci : pour qu'un message soit transmis, deux clés – une publique et l'autre secrète – sont générées par un logiciel. Chaque clé est conservée dans un fichier séparé, appelé « porte-clés », lequel est détenu par chaque usager. Deux partenaires qui désirent communiquer ensemble doivent échanger leur clé publique. L'expéditeur peut utiliser la clé publique du récepteur pour chiffrer le message, et ce dernier va le déchiffrer au moyen de sa clé privée ; ainsi, l'expéditeur s'assure que le récepteur a bel et bien reçu un message intact. À l'inverse, l'expéditeur peut chiffrer le message au moyen de sa clé privée, et le récepteur le déchiffrer avec sa clé publique, ce qui permet d'assurer la confidentialité de l'expéditeur. Enfin, la situation idéale est que les deux partenaires utilisent des clés secrètes, auquel cas il s'agit d'un système de cryptographie à clé privée, ce qui n'est pas transposable dans un réseau ouvert comme Internet. L'avantage majeur du système de cryptographie à clé publique est qu'il permet à deux personnes de conserver la confidentialité

La certification par la cryptographie à clé publique exige la présence d'une autorité de certification, parfois appelée « réseau à valeur ajoutée », laquelle a pour rôle essentiel d'authentifier l'origine du détenteur d'une clé. L'autorité de certification remplit plusieurs fonctions qui gravitent autour de l'authentification des documents et des messages, comme de garantir leur contenu, le moment et le lieu de leur délivrance, leur sécurité et la préservation du message[14] et la délivrance d'un certificat[15]. L'exécution de ces fonctions dépend principalement de l'indépendance de l'autorité de certification par rapport aux intérêts des partenaires et, à un degré moindre, de la participation, financière ou non, d'une chambre de commerce[16].

L'importance de la certification est particulièrement notable dans les environnements ouverts, comme le mentionnent deux auteurs : « *However*, [Trusted Third Parties] *services in the financial sector will not only be useful in pure financial EDI environments, but also within electronic banking relationships (already widespread in Europe), cash withdrawals via ATM's, insurance and use of electronic purses and (international) payment systems between banks*[17] ». En pratique, il

---

dans leurs communications : la clé privée est conservée par le détenteur, tandis que la clé publique est distribuée ouvertement ; de plus, il est mathématiquement impossible pour quiconque de découvrir la clé privée à partir de la clé publique, ce qui représente un avantage majeur. Voir : Jane KAUFMAN WINN, « Couriers Without Luggage: Negotiable Instruments and Digital Signatures », 49 *S.C. L. Rev.* 739, 763 et 764 (1998) ; A. Michael FROOMKIN, « The Essential Role of Trusted Third Parties in Electronic Commerce », 75 *Oregon L. Rev.* 49, 51-53 (1996).

14 H. FRANKEN, « Position and Liabilities of Trusted Third Parties », (1995) 2 *EDI L. Rev.* 85.

15 Celui-ci se définit comme un « document électronique dont l'objet est d'établir un lien entre une personne et une paire de clés asymétriques » : Serge PARISIEN et Pierre TRUDEL, *L'identification et la certification dans le commerce électronique – droit, sécurité, audit et technologies*, Cowansville, Éditions Yvon Blais, 1996, p. 125. Il fournit une variété d'informations au sujet du détenteur. D'autres fonctions ont trait à la conservation des documents ainsi qu'à la création et à la détention des clés.

16 Au surplus, il serait intéressant d'y retrouver une « *free position facing bankruptcy situations of EDI-partners and the tax authorities* », de même qu'une protection contre les recours judiciaires : A.M. FROOMKIN, *loc. cit.*, note 13, 85 et 86. En pratique, nous croyons que ces deux conditions peuvent difficilement être réalisées.

17 Anne-Marie Ch. KEMNA et Herman ROSS, « Results from TEDIS EDIPLAY: The Role and Future of Trusted Third Parties in Payment Systems », (1995) 2 *EDI L. Rev.* 89, 91.

est préférable pour les parties de spécifier dans leur contrat de base qu'elles entendent utiliser les services d'une autorité de certification, puisque l'encadrement juridique demeure incertain.

B. Les tentatives de solution

Simple en apparence, la certification pose plusieurs problèmes d'ordre juridique et technique. En premier lieu, nous présentons les tentatives de solution juridique (1). En second lieu, nous décrivons les récentes techniques qui permettront d'améliorer les lacunes existantes (2).

1. Les tentatives de solution juridique

L'encadrement des transactions en ligne a longtemps été caractérisé par diverses formes d'autorégulation, que ce soit des lignes directrices ou des lois modèles. Bien que plusieurs législateurs aient adopté des mesures de protection dans le domaine du commerce électronique – et des signatures électroniques –, l'autorégulation conserve une certaine importance, ne serait-ce que pour combler les lacunes juridiques. Ce mode normatif a évolué vers un encadrement réglementaire au fil des ans. Nous présentons ces deux formes de régulation de niveau international (a), européen (b) et national (c).

a. La régulation internationale

Jusqu'à la fin des années '90, les internautes prônaient l'absence d'une intervention législative pour encadrer leurs activités. À cette époque, cette approche était justifiée, dans une certaine mesure, par le faible nombre d'usagers. En fait, la majorité des auteurs opinent que des usages propres au cyberespace, parfois appelés *lex electronica*, se sont développés depuis cette période, et qu'ils tendent à se cristalliser rapidement[18]. La popularité sans cesse croissante et, surtout, les litiges qui suivirent, appelèrent à un encadrement législatif[19]. Des organismes internationaux, telles l'Organisation de coopération et de développement économiques (ci-après citée

---

18 Serge PARISIEN, « Un essai sur le mode de formation des normes dans le commerce électronique », (1996) 2 (1) *Lex Electronica*, en ligne : [http://www.lex-electronica.org/articles/v2-1/parisien.html].

19 *Supra*, I.B.1.

« OCDE ») et la Commission des Nations Unies pour le droit commercial international (ci-après citée « CNUDCI »), ont proposé une série de règles destinées à guider les législateurs nationaux. Dans les faits, la législation nationale demeure lacunaire et doit être complétée tant par les formes d'autorégulation que par les usages, comme le précise l'article 1426 C.c.Q., lorsque le contrat est silencieux ou imprécis.

En ce qui concerne les travaux internationaux touchant la certification, la CNUDCI a adopté deux lois types qui ont connu un franc succès. Après avoir adopté la *Loi type de la CNUDCI sur le commerce électronique*[20] en 1996, la CNUDCI a approfondi les questions relatives aux signatures électroniques et à la certification dans la *Loi type de la CNUDCI sur les signatures électroniques*[21], laquelle est destinée à compléter la loi type de 1996 en tant qu'instrument juridique distinct[22]. L'article premier de la *Loi type de la CNUDCI sur les signatures électroniques*[23] en détermine l'étendue, en mentionnant que la loi type « s'applique lorsque des signatures électroniques sont

---

20 CNUDCI, « *Loi type de la CNUDCI sur le commerce électronique* », A/51/17, dans CNUDCI, *Annuaire de la Commission des Nations Unies sur le droit commercial international*, t. XXVII, 1996, New York, 28 mai-14 juin 1996, A/51/17, Annexe I, p. 247.

21 CNUDCI, « *Loi type de la CNUDCI sur les signatures électroniques* », dans *Projet de guide pour l'incorporation dans le droit interne de la* Loi type de la CNUDCI sur les signatures électroniques, Vienne, 25 juin-13 juillet 2001, A/CN.9/493, Annexe, en ligne : [http://www.uncitral.org/fr-index.htm] (ci-après cité « *Projet de guide* »).

22 *Projet de guide*, *op. cit.*, note 21, nº 65, p. 29. La CNUDCI se penche depuis quelques années sur l'élaboration de règles uniformes pour la réglementation des signatures électroniques : *id.* ; CNUDCI, « Projet de Loi type de la CNUDCI sur les signatures électronique », dans *Rapport du Groupe de travail sur le commerce électronique sur les travaux de sa trente-septième session*, Vienne, 18-29 septembre 2000, A/CN.9/483, Annexe, en ligne : [http://www.uncitral.org/fr-index.htm]. L'idée de réglementer les signatures électroniques et les autorités de certification est apparue en 1996 lorsque la CNUDCI a approché le Groupe de travail sur le commerce électronique à ce sujet : CNUDCI, « Rapport de la Commission des Nations Unies sur le droit commercial international sur les travaux de sa vingt et unième session », dans *Annuaire de la Commission des Nations Unies sur le droit commercial international*, *op. cit.*, note 21, nº 17. L'ensemble des documents préparatoires est disponible dans le site Internet de la CNUDCI : CNUDCI, *Documents préparatoires sur les signatures électroniques*, en ligne : [http://www.uncitral.org/fr-index.htm].

23 CNUDCI, « *Loi type de la CNUDCI sur les signatures électroniques* », dans *Projet de guide*, *op. cit.*, note 21, Annexe.

utilisées dans le contexte d'activités commerciales. Elle ne se substitue à aucune règle de droit visant à protéger le consommateur »[24]. Ainsi, ce projet n'exclut aucunement la protection des consommateurs[25], mais il reconnaît que les législations qui ont pour objet la protection des consommateurs peuvent avoir préséance sur la loi type[26]. Les articles 8, 9 et 11 de la *Loi type de la CNUDCI sur les signatures électroniques* traitent des normes de conduite du signataire, du prestataire de services de certification – autorité de certification – et de la partie qui se fie à la signature ou au certificat. Nous sommes d'avis que ces dispositions couvrent les activités des autorités de certification de niveau supérieur. En effet, la loi type définit le « prestataire de services de certification » en faisant référence à « une personne qui émet des certificats et peut fournir d'autres services liés aux signatures électroniques »[27]. Or, la supervision par une autorité de certification de niveau supérieur vis-à-vis du prestataire de services de certification de niveau subalterne exige l'émission d'un certificat. Ce processus doit être accompli pour chaque niveau intermédiaire jusqu'au niveau ultime.

En novembre 2005, la CNUDCI a adopté la *Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux*[28]. Cette convention vise, notamment, les critères qui permettent d'établir l'équivalence fonctionnelle entre les communications électroniques et les documents sur support traditionnel – incluant les documents « originaux » – et entre les techniques d'authentification électronique et les signatures manuscrites.

---

24 Le champ d'application s'aligne sur la *Loi type sur le commerce électronique*. La CNUDCI ajoute que le terme « commerciales » s'interprète au sens large et comprend notamment les investissements, le financement et les opérations bancaires : *Projet de guide*, *op. cit.*, note 21, n° 87, p. 37.

25 Tel est le cas pour d'autres modèles de loi de la CNUDCI : CNUDCI, « *Loi type de la CNUDCI sur les virements internationaux* », dans *Annuaire de la Commission des Nations Unies sur le droit commercial international*, t. XXIII, 1992, New York, 14 mai-22 juin 1992, A/CN.9/346, Annexe II, p. 437, et la *Loi type de la CNUDCI sur le commerce électronique*, précitée, note 20.

26 *Projet de guide*, *op. cit.*, note 21, n° 91, p. 38.

27 Art. 2, *Loi type de la CNUDCI sur les signatures électroniques*, précitée, note 21.

28 CNUDCI, *Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux*, Doc. off. AG CNUDCI, 60e sess., supp. n° 17, Annexe 1, Doc. NU A/60/17 (2005) (ci-après citée « *Convention sur l'utilisation de communications électroniques* »). Voir : John D. GREGORY, « The Proposed UNCITRAL Convention on Electronic Contracts », (2003) 59 *Bus. Law.* 313.

En fait, cette convention, qui ne s'applique qu'aux transactions commerciales[29] internationales[30], ne traite pas directement de l'authentification. Elle prévoit l'équivalence d'une signature électronique lorsque les exigences d'intégrité sont présentes[31].

b. La régulation européenne

En mai 1998, la Commission européenne a présenté une proposition de directive afin d'instaurer un cadre commun pour les signatures électroniques[32]. Cette proposition a été arrêtée par le Parlement européen et le Conseil de l'Union européenne en décembre 1999[33]. La Directive 1999/93/CE a été complétée quelques années plus tard par la *Décision de la Commission du 14 juillet 2003 relative à la publication des numéros de référence de normes généralement admises pour les produits de signatures électroniques conformément à la directive 1999/93/CE du Parlement européen et du Conseil (Texte présentant de l'intérêt pour l'EEE)*[34]. La *Directive 1999/93/CE* vise l'établissement d'un environnement juridique fiable pour l'utilisation des signatures électroniques et leur reconnaissance juridique dans le but de renforcer la confiance des usagers dans les signatures électroniques[35]. Elle encadre donc le développement des activités des prestataires de service de certification sur des réseaux ouverts[36].

---

29 L'article 2(1)(a) de la *Convention sur l'utilisation de communications électroniques*, précitée, note 28, prévoit l'exclusion des « [c]ontrats conclus à des fins personnelles, familiales ou domestiques ».

30 *Id.*, art. 1(1).

31 *Id.*, art. 9.

32 CE, *Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques*, [1998] J.O. C. 325/5, adoptée par la Commission en mai 1998 (ci-après citée « *Proposition 325/5* »).

33 CE, *Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques*, [2000] J.O. L. 13/12 (ci-après citée « *Directive 1999/93/CE* »).

34 [2003] J.O. L. 175/45. Cette directive ne représente qu'une simple mise à jour de la liste des normes généralement admises pour les produits de signatures électroniques dont les États membres présument qu'ils sont conformes aux exigences visées à l'Annexe II(f), de la *Directive 1999/93/CE*.

35 *Directive 1999/93/CE*, précitée, note 33, Préambule, par. 4, art. 1.

36 *Id.*, Préambule, par. 4. La *Proposition 325/5*, précitée, prévoyait explicitement l'importance d'harmoniser les règles des autorités de certification, car « des différences dans le champ d'application et le contenu de ces réglementations

La *Directive 1999/93/CE* suggère deux définitions de la signature électronique, soit la simple «signature électronique» et la « signature électronique avancée »[37]. La première est décrite comme « une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification », tandis que la seconde représente une signature électronique qui respecte des critères précis : « être liée uniquement au signataire[,] permettre d'identifier le signataire[,] être créée par des moyens que le signataire puisse garder sous son contrôle exclusif et [...] être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable »[38]. La directive reconnaît le caractère international du commerce électronique en favorisant l'accès au marché dans les États membres (art. 3) et la reconnaissance des certificats émis par un prestataire d'un État par un autre État membre (art. 7). Les détails techniques concernant la certification sont prévus dans les annexes : les caractéristiques des certificats (Annexe 1) ; les fonctions et les responsabilités des prestataires de service de certification (Annexe 2) ; les exigences pour les dispositifs sécurisés de création de signature électronique (Annexe 3) et les recommandations pour la vérification sécurisée de la signature (Annexe 4).

c. La régulation nationale

Au Canada, la Conférence pour l'harmonisation des lois au Canada (ci-après citée « Conférence ») a préparé la *Loi uniforme sur*

---

risquent de susciter des incertitudes juridiques », ce qui pourrait porter préjudice au « commerce transfrontalier et [entraver] le bon fonctionnement du marché intérieur » : *Proposition 325/5*, précitée, note 32, préambule, par. 5, 7, et 11. Le Parlement et le Conseil ne reprennent pas en détail cette philosophie, mais ils la sous-entendent dans le préambule. Notamment, voir les paragraphes 5 et 20 du préambule de la *Proposition 325/5*, *id.* Toutefois, le paragraphe 17 affirme que l'harmonisation ne doit pas porter « atteinte aux obligations d'ordre formel instituées par le droit national pour la conclusion de contrats ni aux règles déterminant le lieu où un contrat est conclu ».

37 *Directive 1999/93/CE*, précitée, note 33, art. 2(1)(2). Toutefois, la *Proposition 325/5*, précitée, note 32, précédant la *Directive 1999/93/CE*, ne l'avait point retenue.

38 Voir l'analogie avec la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5.

le commerce électronique[39] en 1999. Cette loi uniforme se divise en trois parties, soit la fourniture et la conservation de l'information, qui présentent des règles de base analogues à celles de la *Loi type sur le commerce électronique*, la communication de documents électroniques et le transport de marchandises. La *Loi uniforme sur le commerce électronique* est principalement orientée vers la reconnaissance des documents électroniques et ne traite que partiellement de la signature électronique. La certification est donc exclue de cette loi uniforme. En fait, celle-ci s'est inspirée de la *Loi type de la CNUDCI sur le commerce électronique*[40] pour en implanter les principes fondamentaux[41]. Destinée aux législateurs canadiens, les gouvernements provinciaux de l'extérieur du Québec ont codifié cette loi uniforme, en tout ou en partie, dans leur corpus législatif[42], tandis que le gouvernement fédéral a choisi d'adopter la *Loi sur la protection des renseignements personnels et les documents électroniques*[43], qui admet la simple signature électronique et la signature électronique sécurisée.

Le Québec fait cavalier seul, en quelque sorte, puisqu'il a adopté la *Loi concernant le cadre juridique des technologies de l'information*[44],

---

39 CONFÉRENCE POUR L'HARMONISATION DES LOIS AU CANADA, *Loi uniforme sur le commerce électronique*, Ottawa, août 1999, en ligne : [http://www.ulcc.ca/fr/us].

40 Précitée, note 20.

41 Précitée, note 39.

42 Alberta : *Electronic Transactions Act*, R.S.A. c. E-5.5, entrée en vigueur le 1er avril 2003 ; Colombie-Britannique : *Electronic Transactions Act*, S.B.C. (2001), c. 10, sanctionnée le 11 avril 2001 ; Île-du-Prince-Édouard : *Electronic Commerce Act*, R.S.P.E.I. (1988), c. E-4.1, entrée en vigueur le 15 mai 2001 ; Manitoba : *Loi sur le commerce et l'information électroniques*, C.P.L.M., c. E-55, entrée en vigueur le 18 août 2000 ; Nouveau-Brunswick : *Loi sur les opérations électroniques*, L.R.N.B., c. E-5.5, entrée en vigueur le 31 mars 2002 ; Nouvelle-Écosse : *Electronic Commerce Act*, N.S.S. (2000), c. 26, entrée en vigueur le 1er décembre 2000 ; Ontario : *Loi de 2000 sur le commerce électronique*, L.O. (2000), c. 17, entrée en vigueur le 16 octobre 2000 ; Saskatchewan : *Electronic Information and Documents Act*, R.S.S. (2000), c. E-7.22, entrée en vigueur le 1er novembre 2000 ; Terre-Neuve : *Electronic Commerce Act*, S.N.L. (2001), c. E-5.1, sanctionnée le 13 décembre 2001 ; Yukon : *Loi sur le commerce électronique*, R.S.Y. (2002), c. 66, entrée en vigueur le 27 mai 2000.

43 Précitée, note 38.

44 Précitée, note 1.

qui vise la reconnaissance juridique des documents informatisés[45]. Cette loi, qui complète le *Code civil du Québec*[46], encadre, notamment, les activités des autorités de certification en précisant les caractéristiques d'un certificat et du répertoire destiné à l'archivage, l'énoncé de politique de l'autorité de certification et les droits et les obligations des parties[47]. À l'instar de la *Loi type de la CNUDCI sur les signatures électroniques*[48], nous sommes d'avis que la loi québécoise encadre les autorités de certification de niveau supérieur.

Afin de bien comprendre l'importance des signatures électroniques, il est intéressant d'analyser brièvement la situation étatsunienne. En 1996, l'American Bar Association (ci-après citée « ABA ») a présenté un projet de lignes directrices destiné à gouverner les signatures électroniques, appelé *Digital Signature Guidelines*[49]. Les ABA Guidelines ont pour objet d'établir une relation juridique entre les autorités de certification, les signataires ainsi que les personnes se fiant à une signature et à un certificat[50]. Contrairement à la *Loi uniforme sur le commerce électronique*[51], ces lignes directrices n'ont pas été produites dans le but d'être adoptées formellement par le législateur, mais elles doivent être perçues comme un point de départ pour l'harmonisation des principes juridiques et peuvent être utilisées en tant que « *common basis for more precise rules in various legal systems* »[52]. Contrairement à la *Loi uniforme sur le commerce*

---

45 Les premières décisions confirment l'esprit de cette loi : *Vandal* c. *Salvas*, B.E. 2006BE-13 (C.Q.) ; *La Citadelle, compagnie d'assurances générales* c. *Communauté urbaine de Montréal (Ville de Montréal)*, J.E. 2005-1418, EYB 2005-92745 (C.S.) ; *Les entreprises Robert Mazeroll Ltée* c. *Expertech – Bâtisseur de réseaux Inc.*, C.Q. Mingan, nº 650-22-001933-049, 5 janvier 2005, j. Guylaine Tremblay.

46 Art. 2837-2842 C.c.Q., modifiés en 2001 par la *Loi concernant le cadre juridique des technologies de l'information*, L.Q. 2001, c. 32, art. 78 (l'article 78 est omis dans la version des lois refondues).

47 Précitée, note 1, art. 47-62. Nous traiterons du volet responsabilité en seconde partie de ce texte, à la section II.B.

48 Précitée, note 21.

49 SECTION OF SCIENCE AND TECHNOLOGY, ELECTRONIC COMMERCE DIVISION, INFORMATION SECURITY COMMITTEE (ABA), *Digital Signature Guidelines*, Chicago, 1996, en ligne : [http://www.abanet.org/scitech/ec/isc/dsg-toc.html] (ci-après citées « ABA Guidelines »).

50 ABA Guidelines, *op. cit.*, note 49, p. 22.

51 Précitée, note 39.

52 ABA Guidelines, *op. cit.*, note 49, p. 22 et 23.

électronique[53], les ABA Guidelines sont essentiellement orientées vers les signatures digitales et non vers les signatures électroniques[54].

Les ABA Guidelines ont favorisé l'éclosion de plusieurs législations états-uniennes[55], dont la pionnière, l'*Utah Digital Signature Act*[56]. Cette loi était destinée à reconnaître les signatures digitales et les documents électroniques. Contrairement à la loi québécoise, qui favorise la neutralité technologique, la loi de l'Utah n'admettait qu'une seule méthode, soit la cryptographie à clé publique, ce qui a soulevé quelques inquiétudes lors de son adoption[57]. En mai 2006, cette loi a été presque entièrement abrogée pour éliminer, entre autres, cette lacune et adopter la neutralité technologique[58]. Il est intéressant de noter que, contrairement à la *Loi type de la CNUDCI sur les signatures électroniques*[59], à la Directive 1999/93/CE[60] ou aux ABA Guidelines[61], l'*Utah Digital Signature Act* spécifiait en détail la manière dont une autorité de certification devait procéder pour obtenir une licence[62].

---

53 Précitée, note 39.

54 *Id.*, note 49, p. 21. Les signatures digitales ont trait à la cryptographie asymétrique ; les signatures électroniques proviennent de technologies plus variées. Voir : Edward D. KANIA, « The ABA's Digital Signature Guidelines: An Imperfect Solution to Digital Signatures on the Internet », (1999) 7 *Comm. Law Conspectus* 297, 301.

55 Voir à titre d'exemple : Californie : *California Digital Signature Act*, Cal. Civ. Code Ann. § 1633.2 (West 2001) et *California Signature Regulations*, Cal. Code Reg. § 22000 (West 1998) ; Floride : *Electronic Signature Act of 1996*, Fla. Stat. § 668.001 (West 2000) ; New York : *Electronic Signatures and Records Act*, NY State Tech § 101 (McKinney, 2001) ; Virginie : *Uniform Computer Information Transactions Act*, Va. Code Ann. § 59.1-501.1 (West 2001).

56 *Utah Code* §§ 46-3-101 – 46-3-504, L. 1995, c. 61, Utah Code Ann. Tit 46 (1995) (ci-après citée « *Utah Digital Signature Act* »). Dans le cas de cette loi, l'influence des ABA Guidelines vient des travaux préliminaires de ces lignes directrices.

57 S. PARISIEN, *loc. cit.*, note 18, 2.

58 *Repeal of Utah Digital Signature Act*, Bill S. 20, Utah State Leg., 2006 Gen. Sess. (Ut., 2006), en ligne : [http://www.le.state.ut.us/~2006/bills/sbillint/sb0020.htm].

59 Précitée, note 21.

60 Directive 1999/93/CE, précitée, note 33.

61 ABA Guidelines, précitées, note 49.

62 *Utah Digital Signature Act*, précitée, note 56, §§ 46-3-201 – 46-3-204. Voir *infra*, note 210, et le texte correspondant.

2. Les tentatives de solution technique

Les progrès de la technologie apportent un éclairage nouveau pour tenter de résoudre les lacunes de la sécurité. Nous analysons les principales méthodes prometteuses, soit le protocole de communication sécurisée *Secure Sockets Layer* (ci-après cité « SSL ») (a), la labellisation (b) et la certification croisée (c). Nous survolons ensuite les développements à l'échelle internationale (d).

a. Le protocole de communication sécurisée SSL

Le type de connexion sécurisée le plus courant dans Internet est le *Secure Sockets Layer*[63]. Il s'agit d'un protocole d'authentification et de chiffrement permettant une communication sécurisée utilisant la cryptographie asymétrique. Introduit en 1994, le SSL devient rapidement le standard de sécurité *de facto* du commerce électronique[64]. Le SSL se retrouve dans les transactions bancaires en ligne, dans les entreprises d'achat en ligne[65] et dans les Intranets de compagnies ou de groupes d'utilisateurs/abonnés à un service[66]. La liaison sécurisée par le SSL est identifiée par une icône de sécurité[67] donnant accès à un certificat contenant des informations sur le site certifié, le champ d'action pour lequel le certificat est émis, l'État dans lequel il est émis et le nom de l'autorité de certification émettrice et l'identification du certificat racine de cette autorité[68]. Lors de chaque connexion, le SSL génère une clé aléatoire et un canal de communication sécurisé. Sa fiabilité tient notamment à

---

63 Tomasz ONYSZKO, « Secure Socket Layer », *Authentication, Access Control & Encryption*, TechGenix WindowSecurity, 2002, mis à jour 2004, en ligne : [http://www.windowsecurity.com/articles/Secure_Socket_Layer.html].

64 Sean M. KERNER, « SSL: Your Key to E-Commerce Security », (2005) *E-Commerce Guide*, en ligne : [http://www.ecommerce-guide.com/solutions/secure_pay/article.php/3510761]. La situation perdure encore aujourd'hui.

65 À titre d'exemple, les achats en ligne d'Amazon, d'Archambault, de Future Shop, d'E-bay, de Paypal et de plusieurs autres.

66 Notamment, l'accès à une version électronique d'un quotidien par les abonnés en ligne, comme le cas des journaux distribués par Cyberpresse. Voir le site de cette entreprise : [http://www.cyberpresse.ca].

67 Sur Netscape, Internet Explorer et Maxthon, un cadenas doré fermé dans le bas droit de l'écran illustre une communication sécurisée. Sur Mozilla Firefox, il s'agit d'une clé argentée dans un cercle vert dans le bas droit de l'écran, et sur Safari, il s'agit d'un petit cadenas gris dans le haut de la page, à l'extrême droite de l'écran.

68 S.M. KERNER, *loc. cit.*, note 64.

cette clé, car bien qu'un pirate informatique puisse découvrir la clé utilisée lors de la dernière connexion, celle-ci ne lui sera d'aucune utilité puisque la connexion suivante générera une clé différente[69].

Les usages courants du SSL constituent des connexions de courte durée : le temps d'une transaction en ligne, d'une opération bancaire en ligne et de la consultation de courriels sécurisés. Il est donc impossible en une courte période de déchiffrer les clés et de pénétrer dans la connexion sécurisée. Cependant, des chercheurs de l'École polytechnique fédérale de Lausanne ont contourné la sécurité du SSL en 2003[70]. Malgré cette expérience, il est toujours considéré comme la meilleure option de sécurisation des transactions, vu que les connexions sécurisées sont destinées à de courtes séances[71]. Le SSL demeure donc hautement sécuritaire pour des connexions de courtes durées telles que les transactions bancaires en ligne. Pour transgresser le SSL, le pirate doit savoir à quel moment sa victime se connectera et cette dernière doit maintenir une connexion d'une durée suffisamment longue. D'ailleurs, par souci de protection supplémentaire, plusieurs sites de transactions en ligne contiennent une procédure de fermeture de session sécurisée automatique en cas d'inactivité prolongée.

b. La labellisation

La labellisation des sites Web constitue un des meilleurs moyens de rassurer les utilisateurs de ces sites et d'assurer une plus grande sécurité dans les transactions en ligne. Qualifiée à la fois de moyen

---

69 T. ONYSZKO, *loc. cit.*, note 63.

70 La violation de la clé par ces chercheurs était expérimentale. Les chercheurs de Lausanne n'ont pas attaqué les algorithmes de chiffrement couramment utilisés par les navigateurs Web et ils précisent que les conclusions de l'expérience ne peuvent s'appliquer au chiffrement utilisé par les navigateurs commerciaux : Estelle DUMONT, « Sécurité : Une faille mise à jour dans le protocole SSL », *ZDNet France* (21 février 2003), en ligne : [http://www.zdnet.fr/actualites/informatique/0,39040745,2130830,00.htm]. Voir également : ASSOCIATED PRESS, « Des failles dans un protocole de sécurité d'Internet », *La Presse*, Montréal, 21 février 2003, B4.

71 Ceci dans l'hypothèse où ce dernier contient 128 bits. Ces chiffres tiennent évidemment compte de la technologie actuelle. Le SSL s'est perfectionné depuis cette expérience. Verisign annonce qu'environ un trillion d'années d'attaques répétées sont nécessaires pour pénétrer le SSL actuel. Voir : VERISIGN, « Comment offrir le cryptage SSL le plus fiable du marché », Mountain View, Verisign, 2004, 2, en ligne : [http://www.verisign.fr/static/030138.pdf].

technique et juridique, la labellisation consiste à fournir une garantie de qualité par un engagement à se conformer à certains critères établis par la législation applicable, par le tiers labellisateur ou par les politiques internes d'un site se labellisant lui-même[72]. Cette pratique regroupe diverses techniques allant de la labellisation interne, sans l'intervention d'un tiers à la labellisation externe, totalement assurée par un tiers, en passant par toute la gamme de degrés d'intervention du tiers située entre ces deux extrêmes. Utilisée dans divers domaines, dont l'environnement[73], cette technique convient très bien au problème soulevé en espèce.

À l'instar de la certification, qui offre un degré de fiabilité variable selon le type de vérifications effectuées par l'autorité de certification préalablement à la délivrance d'un certificat[74], la labellisation de sites offre également divers degrés de fiabilité[75]. Ainsi, l'éducation et la sensibilisation des usagers apparaissent comme étant des facteurs importants de l'implantation d'un réseau ouvert sécuritaire[76].

---

72 Séverine DUSOLLIER et Laetitia ROLIN JACQUEMYNS, « Le défi du droit face au commerce électronique : Les initiatives de l'Union Européenne », (2000) 5-1 *Systèmes d'information et Management* 1, 9 ; Didier GOBERT et Anne SALAÜN, « La labellisation des sites Web : Classification, stratégies et recommandations », (1999) 51 *DAOR* 83, en ligne : [http://www.droit-technologie.org/dossiers/labellisation_web_classification_strategies.pdf], p. 2 (les pages indiquées sont celles du document en ligne).

73 Plus précisément, il s'agit de l'étiquetage des produits contenant des organismes génétiquement modifiés, mieux connus sous le nom d'OGM. Voir généralement : Louis-Philippe LAMPRON, *L'encadrement juridique de la publicité et de l'étiquetage écologiques : une voie vers la mise en œuvre du développement durable au Canada ?*, mémoire de maîtrise, Québec, Faculté des études supérieures, Université Laval, 2004.

74 Voir à cet effet les divers types de certificats offerts par l'autorité de certification Verisign, en ligne : [http://www.verisign.com/repository/disclosure.html].

75 Certains labels garantissent le respect d'une condition particulière telle la protection de la vie privée et des renseignements personnels, alors que d'autres peuvent garantir un ensemble de politiques, procédures, engagements et responsabilités du site labellisé : AICPA, *Suitable Trust Services Criteria ans Illustrations*, New York, AICPA, 2003, p. 3, en ligne : [http://www.webtrust.org/download/final-Trust-Services.pdf].

76 TRUSTe fait appel aux Internautes pour rapporter les usages abusifs ou frauduleux du label, ce qui implique que l'internaute consulte le label délivré et le site du labellisateur afin de connaître l'existence de ce programme. Voir à ce sujet le site Internet du labellisateur, en ligne : [http://www.truste.org/consumers/privacy_alert.php].

Dans le premier cas, la labellisation interne constitue l'initiative d'un site – appelé site candidat – qui propose un engagement à respecter certains critères définis. Elle ne s'accompagne ni d'un contrôle préalable ni de vérifications périodiques par un organisme tiers indépendant[77]. Il existe plusieurs niveaux de sécurité dans la labellisation interne. La labellisation de premier niveau offre le degré de sécurité le plus faible. Les critères labellisés sont déterminés par le site candidat et affichés pour consultation par les utilisateurs[78]. À titre d'exemple, au Canada, la Banque Nationale offre le service « garantie tranquillité d'esprit »[79] alors que la RBC Banque Royale propose le sceau « garantie de sécurité, RBC Banque en direct »[80]. Ces garanties accordent un meilleur service de sécurité et de remboursement tant en cas de transaction frauduleuse ou défectueuse qu'en l'absence de garantie. La labellisation de deuxième niveau permet un niveau de sécurité légèrement plus élevé, puisqu'un tiers indépendant intervient de façon passive dans la rédaction des critères à garantir. Le choix de ces critères n'est donc pas laissé à l'entière discrétion du site candidat. Comme pour le premier niveau, les critères garantis sont affichés sur le site candidat pour consultation[81]. La labellisation de troisième niveau est équivalente à la précédente, mais elle est renforcée par un mécanisme de réception et de traitement des plaintes fourni et opéré par le site candidat[82]. Selon la qualité de la gestion de ce mécanisme, il est possible que l'usager se sente faussement protégé par un mécanisme de règlement des plaintes qui s'avère inefficace[83]. Le traitement des plaintes et du règlement de celles-ci par un système de résolution alternative des litiges offre l'avantage de la stabilité et le sérieux de la

---

77 D. GOBERT et A. SALAÜN, *loc. cit.*, note 72, 4.

78 Le site candidat garantit alors les aspects qu'il détermine lui-même et seulement ces aspects : *id.*, 6 et 10.

79 BANQUE NATIONALE DU CANADA, « Un gage de sécurité assurée ! », 2006, en ligne : [http://www.bnc.ca/bnc/cda/productfamily/0,1010,divId-2_langId-2_navCode-804,00.html].

80 RBC BANQUE ROYALE, « Faites vos opérations bancaires en ligne en toute confiance », 2006, en ligne : [http://www.rbcbanqueroyale.com/endirect/rbcbanqueendirect.html].

81 D. GOBERT et A. SALAÜN, *loc. cit.,* note 72, 6 et 11.

82 *Id.,* 6 et 12.

83 *Id.*, 13.

démarche, mais il risque d'augmenter substantiellement les coûts pour le site candidat[84].

Dans le second cas, la labellisation externe se caractérise d'abord par le concours actif d'un tiers indépendant. Cette intervention se fait en deux temps, soit par une vérification préalable du respect des critères précédant l'octroi du label et par une vérification *a posteriori*, sur une base périodique ou à la suite d'une plainte d'un utilisateur[85]. La labellisation de quatrième niveau est singularisée par un choix des critères à garantir déterminé par le site candidat sans l'intervention d'un tiers. À l'instar du premier niveau, le site candidat choisit lui-même ce qu'il souhaite garantir, et ces critères sont affichés sur le site candidat. Cependant, à la différence du premier niveau, un tiers indépendant interviendra préalablement à l'octroi du label et ensuite de façon périodique afin de s'assurer que les critères choisis soient respectés[86]. Le tiers ne vérifie ni la pertinence ni la qualité des critères identifiés par le site candidat ; il s'assure simplement de leur respect. Les vérifications effectuées par le tiers sont généralement affichées sur le site candidat sous forme de rapport afin d'offrir une image positive à l'internaute. Enfin, le site candidat affiche le logo du tiers indépendant ainsi qu'un lien vers le site de ce dernier afin de souligner son intervention[87]. La labellisation de cinquième niveau constitue la forme la plus fiable et la plus solide qu'il soit. Elle possède toutes les caractéristiques de contrôle et de vérification par un tiers que nous avons identifiées au quatrième niveau. Cependant, dans le cas du cinquième niveau, ce n'est pas le site candidat qui détermine les critères à garantir, mais le tiers indépendant qui intervient aussi de manière active à ce niveau du processus de labellisation[88].

---

84 *Id.* Un système tel que Fin-Net en Europe semble cependant de nature à favoriser cette option, par son sérieux et sa popularité croissante. Voir notamment : Marc LACOURSIÈRE, « Les méthodes alternatives de résolution des conflits au service de la protection des consommateurs de services bancaires en ligne dans les Amériques », (2006) 21 *B.F.L.R.* 357.

85 D. GOBERT et A. SALAÜN, *loc. cit.*, note 72, 7.

86 *Id.*

87 *Id.*, 14.

88 *Id.*, 7 et 15.

À titre d'exemple, Webtrust[89] représente l'illustration idéale de labellisation de cinquième niveau. Les critères à garantir sont élaborés par un groupe d'experts après l'étude des points à renforcer chez le site candidat pour gagner la confiance des usagers[90]. L'octroi du label se fait par la délivrance d'un rapport de certification sans réserve par des experts-comptables et praticiens autorisés par Webtrust, après avoir effectué une analyse des pratiques du site candidat[91]. Il est intéressant de comparer Webtrust avec TRUSTe[92], laquelle permet la labellisation de cinquième niveau, mais se distingue de Webtrust sur plusieurs points. Premièrement, TRUSTe est principalement axée sur la protection de la vie privée des usagers[93]. Deuxièmement, TRUSTe permet au site candidat d'ajouter les critères qu'il désire garantir par son label, ce qui en fait un système hybride entre les quatrième et cinquième niveaux. Troisièmement, la présence d'une autorité de certification n'est pas nécessaire, mais un tiers indépendant agit comme auditeur lors de la demande de label et à titre de surveillant par la suite[94]. Finalement, TRUSTe supporte un mécanisme complet de résolution des litiges pour les usagers. En définitive, les critères TRUSTe sont fondés sur les préoccupations des usagers afin d'établir la confiance pour les transactions dans Internet. TRUSTe permet un équilibre entre la

---

89 Voir le site de Webtrust : [http://www.cpawebtrust.org]. Fondée par l'American Institute of Certified Public Accountants et l'Institut canadien des comptables agréés, les services offerts par WebTrust et SysTrust sont définis comme un ensemble de services professionnels de certification et de conseil fondé sur un cadre commun. Les quatre grands axes de vérification et d'intervention de Webtrust touchent : 1° les politiques du site candidat ; 2° la communication de ces politiques ; 3° les procédures utilisées pour atteindre les objectifs définis dans les politiques et 4° la surveillance du système et la prise de mesures pour assurer le respect des politiques définies : AICPA/ICCA, *Principes et critères des services Trust : Intégration de Systrust et de Webtrust*, AICPA/ICCA, 2003, p. 3, en ligne : [http://www.icca.ca/multimedia/Download_Library/Standards/WebTrust/French/ES_AICPA-CICA_services_trust.pdf].

90 Didier GOBERT et Anne SALAÜN, « La labellisation des sites Web : Inventaire des initiatives existantes », (1999) 35 *Communications et Stratégies* 229, en ligne : [http://www.droit-technologie.org/dossiers/LABELLISATION_WEB_INVENTAIRE.pdf], p. 5 (les pages indiquées sont celles du document en ligne). La liste des critères Webtrust peut être consultée à l'adresse suivante : [http://www.cpawebtrust.org/download/final-Trust-Services.pdf].

91 *Id.*, p. 3 et 5.

92 Voir le site du labellisateur : [http://www.truste.org].

93 D. GOBERT et A. SALAÜN, *loc. cit.*, note 72, 11.

94 Il s'agit présentement des firmes Price Watherhouse Coopers et KPMG : *id.*, 12.

sécurité souhaitée par les usagers et le désir des sites candidats d'être liés à des normes qui découlent de l'autorégulation, ce qui rend moins nécessaire une initiative législative contraignante[95].

Il est fréquent de voir des sites candidats labellisés par un quatrième ou un cinquième niveau offrir une connexion sécurisée à leur clientèle en ligne, notamment par un chiffrement de la transaction et des pages qui contiennent les critères garantis[96]. Une entente *ad hoc* entre le tiers labellisateur et le site candidat de même que des choix stratégiques par le site candidat permettent d'apporter certaines variantes aux niveaux présentés.

À nos yeux, les sites de transactions bancaires en ligne devraient au minimum être labellisés à un quatrième niveau, car la labellisation garantit le respect de politiques de protection de la vie privée, de la sécurité et de la disponibilité des services. La certification utilisée sans label permet de chiffrer la communication serveur-client et de vérifier l'identité du site bancaire, mais n'offre pas la garantie supplémentaire représentée par les audits réguliers nécessaires à la conservation d'un label de quatrième ou cinquième niveau. Actuellement, les grandes banques canadiennes n'utilisent pas de label externe. Bien qu'elles soient supervisées par plusieurs organismes, comme l'Association canadienne des paiements (ci-après citée « ACP ») et le Bureau du surintendant des institutions financières en ce qui a trait aux opérations bancaires en général, il serait bénéfique qu'elles adoptent un label externe dans le but de favoriser la confiance dans les transactions bancaires en ligne.

c. La certification croisée

La certification croisée – également appelée réciproque ou cocertification – représente une entente entre deux autorités de certification indépendantes qui se reconnaissent mutuellement. Cette technique est très avantageuse, car elle favorise la confiance des clients d'une autorité de certification envers celle-ci en lui permettant de communiquer de façon sécuritaire avec les clients de sa propre autorité de certification et avec les clients de l'autorité de certification par-

---

95 *Id.*, 11.

96 C'est le cas notamment de TRUSTe et de BBB OnLine. Ce chiffrement s'effectue par le protocole SSL : *supra*, section I.B.2.A. Voir : D. GOBERT et A. SALAÜN, *loc. cit.*, note 72, 16 ; Voir également, en ligne : [http://www.networkworld.com/details/473.html].

tenaire. Puisque les politiques de certification peuvent varier d'un énoncé de politique à un autre, les deux autorités de certification doivent comparer leurs politiques respectives pour s'assurer de l'équivalence du niveau de confiance entre elles avant d'établir une certification croisée[97]. D'un point de vue technique, il s'agit de créer des « certificats réciproques » entre les deux autorités de certification[98]. Lors de ce processus, les autorités de certification échangent en toute sécurité de l'information sur leurs clés cryptographiques, de sorte que chacune puisse certifier efficacement la fiabilité des clés de l'autre. Pour réussir une certification croisée, les deux autorités de certification doivent avoir une confiance sans réserve dans l'énoncé de politique de l'autre. En ce sens, le lien de reconnaissance va bien au-delà du simple échange d'information sur les clés. Lorsque l'entente est établie, les deux autorités acceptent de se faire confiance et de se fier aux clés et aux certificats émis par l'autre comme si elles les avaient émis elles-mêmes[99]. Les clients relevant d'une autorité de certification peuvent donc implicitement avoir confiance dans les usagers relevant de l'autre autorité de certification[100].

En 1999, le gouvernement canadien a lancé un projet d'infrastructure à clé publique (ci-après citée « ICP »). Dès sa création, cette infrastructure prévoyait la procédure à suivre pour obtenir une cocertification de la part du gouvernement. Les gouvernements provinciaux et certains organismes publics ont profité de l'opportunité pour entrer en contact sécurisé avec le gouvernement fédéral. Bien que ces cocertifications s'appliquent actuellement aux communications administratives et non aux autorités de certification offrant des services aux usagers, elles nous permettent tout de même de

---

97 CENTRE DE CERTIFICATION DU QUÉBEC, « La certification croisée ou réciproque », 2006, Montréal, Notarius (CDNQ), en ligne : [http://www.notarius.com/public/ccq/ccq.html].

98 CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS, *Infrastructure à clé publique du gouvernement du Canada – Livre Blanc*, Ottawa, Gouvernement du Canada, 1998, p. 8, en ligne : [http://www.cse-cst.gc.ca/documents/services/mg15af.pdf].

99 TRAVAUX PUBLICS ET SERVICES GOUVERNEMENTAUX CANADA, « Cocertification », Ottawa, Gouvernement du Canada, 2003, en ligne : [http://www.solutions.gc.ca/pki-icp/crosscert/crosscert_f.asp].

100 CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS, *op. cit.*, note 98, p. 8.

suivre une demande de cocertification[101]. Les quatre phases de cocertification applicable à l'infrastructure à clé publique du gouvernement canadien se dessinent comme suit. La phase I est la phase d'initiation du processus[102]. La phase II consiste en un examen des politiques et technologies utilisées par l'autorité de certification demanderesse afin de s'assurer de la compatibilité de celle-ci avec les politiques et technologies de l'infrastructure à clé publique canadienne[103]. La phase III est celle de l'entente[104]. La phase IV s'inscrit dans un but de continuité sous forme de suivi et de vérification périodique du maintien de la compatibilité des politiques de certification[105].

---

101 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *Infrastructure à clé publique du gouvernement du Canada : Méthodologie et critères de cocertification*, Version 1.0, Ottawa, Avril 2000, p. iv, en ligne : [http://www.solutions.gc.ca/pki-icp/crosscert/crosscert_f.pdf].

102 *Id.*, p. 8. L'autorité de certification qui désire être cocertifiée fait sa demande à l'aide des formulaires prescrits accompagnés d'un exemplaire de son énoncé de politique, de ses statuts juridiques et doit démontrer sa capacité financière. Elle doit également être parrainée par un ministère fédéral membre de l'ICP du gouvernement du Canada à l'exception d'une ICP d'un gouvernement étranger : TRAVAUX PUBLICS ET SERVICES GOUVERNEMENTAUX CANADA, *Instaurer la confiance : Cocertification avec l'Infrastructure à clé publique du gouvernement du Canada*, Ottawa, Gouvernement du Canada, 2005, p. 3 et 4, en ligne : [http://www.solutions.gc.ca/pki-icp/crosscert/trust-confiance/trust-confiancepr_f.asp?format=print].

103 TRAVAUX PUBLICS ET SERVICES GOUVERNEMENTAUX CANADA, *op. cit.*, note 102, p. 4 et 5 ; SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *op. cit.*, note 101, p. 12. Sans devoir être identiques, les technologies et politiques doivent être semblables ou équivalentes, c'est-à-dire, offrir le même degré de fiabilité et de sécurité que l'ICP fédérale.

104 Une négociation s'installe entre l'autorité de certification demanderesse et l'ICP du gouvernement canadien. Un projet d'entente est ensuite rédigé et le gouvernement fait ses recommandations à l'autorité de certification demanderesse sous la forme de rapport conditionnel (dans les cas où cette dernière doit modifier certaines pratiques pour être compatible avec l'ICP canadienne) ou inconditionnel. Un rapport inconditionnel conduit à l'établissement de la cocertification alors qu'un rapport conditionnel offre un délai de 20 jours à l'autorité de certification demanderesse pour se conformer aux exigences de l'ICP du gouvernement. Une fois les exigences rencontrées, une période d'essai permet de s'assurer du bon fonctionnement de l'entente. Finalement, la cocertification est annoncée et établie : SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *op. cit.*, note 101, p. 15 et 20 ; TRAVAUX PUBLICS ET SERVICES GOUVERNEMENTAUX CANADA, *op. cit.*, note 102, p. 6.

105 Lorsque la confiance est établie entre l'autorité de certification demanderesse et l'ICP canadienne, il est important de maintenir cette confiance et d'évoluer en

La certification croisée est appelée à prendre de l'ampleur avec l'augmentation graduelle des transactions en ligne[106]. La certification hiérarchique étant coûteuse et peu répandue, la cocertification favorise le développement de la sécurité en ligne en permettant une certaine harmonisation et une plus grande interopérabilité à moindre coût.

La France offre un excellent exemple de certification croisée. En 2001, le ministère de l'Économie, des finances et de l'industrie (ci-après cité « MINÉFI ») a instauré la déclaration de taxe sur la valeur ajoutée par communication électronique[107]. Seize autorités de certification (dont sept opérées par des banques) sont maintenant cocertifiées par le MINÉFI et permettent ainsi à leur clientèle de transmettre leur déclaration de taxe sur la valeur ajoutée par Internet[108]. À l'instar de la France, il est également possible au Canada de transmettre sa déclaration de revenus en ligne. Cependant, à l'instar des sites bancaires, l'autorité de certification intervient à sens unique afin de certifier le site gouvernemental alors que le client s'identifie à l'aide d'une signature numérique (code) non certifiée[109].

---

tandem dans la délivrance et la gestion des certificats. Des rapports de modification sont émis et doivent être respectés par tous les partenaires sous peine de voir résilier l'entente de cocertification. À l'inverse, une autorité de certification ayant respecté tous ses engagements ne devrait pas éprouver de difficulté à renouveler son entente à l'échéance : SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *op. cit.*, note 101, p. 23, 26 et 27 ; TRAVAUX PUBLICS ET SERVICES GOUVERNEMENTAUX CANADA, *op. cit.*, note 102, p. 7.

106 Warwick FORD, « Looking into the Crystal Ball : Certificates Revisited, Presentation at the Worlwide Electronic Commerce Conference », 20 octobre 1995, cité par A.M. FROOMKIN, *loc. cit.*, note 13, 59.

107 NOTE, « La TéléTVA : le paiement de la TVA facilité », (2001) 69 *Industrie* 18, en ligne : [http://www.industrie.gouv.fr/biblioth/docu/kiosque/cahiers/pdf/c0069.pdf].

108 Ces autorités de certification sont : ChamberSign (autorité de certification des Chambres de commerce et d'industrie européennes) ; SG Trust (AC du groupe financier Société Générale) ; BNP Paribas ; Crédit Agricole ; Crédit Lyonnais ; Natexis et Click-n-Trust (AC du groupe financier Banques Populaires) ; HSBC France ; Certinomis ; Certplus ; Greffe-TC-Paris ; Ouverture ; Certigreffe ; Certeurope ; CCF et Atos WORLDLINE. MINÉFI, « Agence autorité du MINÉFI », juillet 2006, en ligne : [http://www.finances.gouv.fr/dematerialisation_icp/dematerialisation_declar.htm].

109 IMPÔTNET, sécurité, en ligne : [http://www.netfile.gc.ca/security-f.html].

d. Les développements internationaux

À ce jour, les autorités de certifications majeures sont principalement des entités commerciales qui offrent leurs services au public, aux entreprises et aux gouvernements[110]. La qualité, la fiabilité et les exigences liées aux certificats émis varient selon les catégories offertes par chaque autorité de certification[111]. La plupart de celles-ci sont présentes dans plusieurs États par l'entremise de partenaires ou de filiales locales. Cela confère un caractère international à la validité des certificats qu'elles émettent sans même avoir recours à la certification croisée[112]. À titre d'exemple, l'acquisition de GeoTrust en mai 2006 a permis à Verisign d'étendre son réseau de certification par le biais des 9000 fournisseurs directs de GeoTrust qui opèrent dans 140 pays[113].

Bien que Verisign soit un acteur de premier plan en matière de certification, d'autres autorités de certification font des démarches sérieuses pour se positionner sur le plan international. IdenTrust[114] a été fondé en 1999 par un consortium bancaire[115]. Il offre les services de sécurisation et de certification à ses membres ainsi qu'à une clientèle d'entreprise et aux particuliers[116]. Surtout actif dans la sécurisation des transactions interentreprises, IdenTrust a mis

---

110 À titre d'exemple : Verisign, Entrust, Identrust, Thawte, Geotrust.

111 Les certificats émis à un organisme gouvernemental sont normalement d'un niveau plus élevé que les certificats offerts aux consommateurs pour sécuriser une messagerie courriel. Voir à titre d'exemple : VERISIGN, « Verisign PKI Disclosure Statement », 2006, en ligne : [https://www.verisign.com/repository/disclosure.html].

112 Pour sa part, Verisign sécurise 3000 entreprises et 450 000 sites Web à l'échelle mondiale et assure une présence marquée sur les cinq continents : VERISIGN, « Where It All Comes Together », (2004) Verisign, Mountain View (CA), p. 8, en ligne : [https://www.verisign.com/static/017579.pdf]. De plus, les autorités de certification Thawte (Afrique, Amérique du Nord, Amérique du Sud), Esign Australia (Australie), Soltrus, Wis@Key (Suisse), et GeoTrust, sont des filiales de Verisign, consolidant sa position de leader mondial.

113 VERISIGN, « Verisign to acquire GeoTrust », *Press release*, 17 mai 2006, en ligne : [http://www.verisign.com/press_releases/pr/page_037923.html].

114 Connue sous les noms de Identrus et IdenTrust, l'autorité de certification a procédé à un changement de nom le 1er mars 2006 pour s'appeler IdenTrust dans tous les aspects de ses services.

115 IDENTRUST, *Company History*, 2006, en ligne : [http://www.identrust.com/company/index.html].

116 Voir à ce sujet, en ligne : [http://www.identrust.com/certificates/index.html].

sur pied le projet Eleanor[117] qui représente une normalisation de messages de paiements interentreprises. À l'instar de Verisign, plusieurs fusions et acquisitions jalonnent son parcours, principalement l'acquisition en 2002 de DigitalSignatureTrust[118]. En 2001, IdenTrust entendait se positionner comme autorité racine d'une hiérarchie de certification mondiale[119]. Dans la hiérarchie envisagée, IdenTrust émet des certificats aux institutions financières clientes qui elles-mêmes émettent des certificats à leurs clients commerciaux. Les institutions financières occupent donc le second niveau dans la hiérarchie de la certification et, puisqu'elles respectent les critères d'IdenTrust, ces institutions financières sont cocertifiées entre elles. Ainsi, le client d'une institution financière est assuré que ses certificats numériques seront reconnus par toutes les institutions financières membres du projet et par tous les clients de ces institutions. Bien que cette hiérarchie ne soit pas totalement opérationnelle, IdenTrust demeure un partenaire certificateur important dans les transactions en ligne outre frontière[120].

De manière plus générale, le Transaction Workflow Innovation Standards Team (ci-après cité « TWIST »), qui travaille en collaboration avec IdenTrust, est un organisme sans but lucratif qui oeuvre principalement à l'harmonisation des normes de communication dans le secteur financier[121]. Depuis plusieurs années, les banques communiquent entre elles par des systèmes de communication spécialisés tels que la Society for Worldwide Interbank Financial Telecommunication (ci-après citée « SWIFT »)[122]. Cependant, avec la croissance rapide de l'utilisation des communications électroniques, les échanges, d'une part, entre la banque et les courtiers et, d'autre part, entre la banque et ses clients, qui se déroulaient principalement par téléphone, se font maintenant couramment par Internet. TWIST vise à créer un environnement standardisé et harmonisé

---

117 IDENTRUS, *ELEANOR, The Complete, Global E-Payments Initiation Solution*, New York, Identrus LLC, 2002, en ligne : [http://www.identrus.com/knowledge_center/pub/Eleanor_Brochure.pdf].

118 Voir à ce sujet, en ligne : [http://www.identrust.com/company/index.html].

119 Renaud HOFFMAN, « Une architecture de certification à l'échelle mondiale », *01net.com* (1er novembre 2001), en ligne : [http://www.01net.com/article/168355.html].

120 IDENTRUST, « We put the Trust in Identity », San Francisco (CA), IdenTrust, 2006, en ligne : [http://www.identrust.com/pdf/IdenTrustBrochure.pdf].

121 Voir à ce sujet, le site de TWIST : [http://www.twiststandards.org].

122 Voir le site Web : [http://www.swift.org].

afin de faciliter ces communications. TWIST travaille également, en collaboration avec l'Organisation internationale de normalisation (ci-après citée « ISO »), sur la création et la gestion de la norme ISO 20022 concernant les communications financières par Internet[123].

Il existe une harmonisation palpable sur le plan international en regard de l'aspect technique de la certification et de la cryptographie à clé publique. L'utilisation généralisée du protocole de communication sécurisée SSL et la part de marché considérable occupée par des autorités de certification telle que Verisign et IdenTrust en sont les principaux facteurs. L'harmonisation permet également de répondre aux besoins de la certification croisée. L'autorité de certification qui désire s'implanter dans un certain milieu adoptera des standards techniques uniformisés afin d'aspirer à une cocertification rapide et peu coûteuse tout en respectant les ententes de cocertification actuelles[124]. À propos de la solution proposée par IdenTrust, Frédéric Pailloux déclarait : « Les banques qui n'ont pas encore rejoint Identrus[t] [...] s'illustrent plus par leur retard ou par une décision stratégique de s'exclure d'un tel système, que par une volonté de proposer une autre solution »[125].

Devant les incertitudes juridiques qui existent aux plans national et international, le marché des autorités de certification s'est créé un corpus de normes et de standards techniques qui visent à pallier ces incertitudes et à assurer le développement de la sécurité Internet. Ces normes et ces standards ont-ils le statut d'usages internationaux ?

---

123 ISO, *ISO 20022 Financial Repository: Business Process Catalogue & Data Dictionary*, ISO, Genève, 2005, en ligne : [http://www.iso20022.org].

124 À titre d'exemple, les certificats acceptés sur une base internationale respectent la norme X509v3 : UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS, « Norme ITU-T X509 », en ligne : [http://www.itu.int/rec/T-REC-X.509/fr] (ci-après citée « UIT »).

125 Cité par R. HOFFMAN, *loc. cit.*, note 119, 2. Rien n'indique qu'un certificat ne respectant pas la norme X509v3 n'est pas tout aussi sécuritaire et fiable. Cependant, il risque fort d'être refusé tant par le cocontractant que l'autorité de certification de celui-ci. De la même manière, un ordre de paiement qui ne rencontre pas les exigences de la norme ISO 20022 utilisant le langage informatique XML risque d'être refusé, malgré que l'ordre de paiement comporte toutes les informations utiles et nécessaires à son exécution : ISO, *op. cit.*, note 123.

La réponse à cette interrogation nécessite un processus en trois étapes[126]. D'abord, il s'agit d'identifier les pratiques en tant que normes. Ensuite, ces normes doivent être institutionnalisées. Enfin, les normes doivent être introduites dans le système juridique interne. Il existe plusieurs exemples de normes techniques qui ont acquis le statut d'usages internationaux, ou s'en rapprochent, que ce soit les normes ISO[127] ou les standards d'échanges de données informatisées, mieux connus sous le nom d'EDI. Dans le domaine bancaire, les règles SWIFT, conçues par un consortium bancaire qui a imposé, en quelque sorte, ses normes de sécurité techniques à l'industrie bancaire internationale, ne peuvent être passées sous silence. Enfin, plus récemment, les banques ont créé une autre forme de standards destinés aux transactions internationales, soit Bolero[128].

Les théories sur la création des normes dans le cyberespace, qui se sont inspirées des travaux de Robert C. Ellickson[129] ainsi que des protagonistes de la nouvelle *lex mercatoria*[130], favorisent une reconnaissance rapide de ces pratiques du cyberespace[131].

3. Les lacunes de la sécurité juridique et technique

La première partie de ce texte permet d'observer les principales démarches complétées depuis quelques années pour atténuer les problèmes qui émanent du manque de sécurité dans Internet. Au fil des ans, les mesures techniques et juridiques se sont interpellées réciproquement. En effet, à la suite de la mise en place de mesures de protection fondées sur des moyens cryptographiques et, parfois, biométriques, certains législateurs sont intervenus pour réguler

---

126 S. PARISIEN, *loc. cit.*, note 18, 3-6.

127 Nabil N. ANTAKI et Charlaine BOUCHARD, *Droit et pratique de l'entreprise*, t. 1, Cowansville, Éditions Yvon Blais, 1999, p. 91.

128 Voir généralement : James Bryce CLARK, « Technical Standards and Their Effects on E-Commerce Contracts: Beyond the Four Corners », (2003) 59 *Bus. Law* 345, 354-357.

129 Robert C. ELLICKSON, *Order without Law: How Neighbors Settle Disputes*, Cambridge (MA), Harvard University Press (1994).

130 Voir généralement : Berthold GOLDMAN, « Frontières du droit et *lex mercatoria* », (1964) 9 *Archives de Philosophie du droit* 177 ; Filali OSMAN, *Les principes généraux de la* lex mercatoria, Paris, L.G.D.J., 1992.

131 S. PARISIEN, *loc. cit.*, note 18, 5.

cette question. À son tour, cet encouragement des autorités gouvernementales a favorisé le perfectionnement des mesures de protection technique.

Une des qualités de la *Loi concernant le cadre juridique des technologies de l'information*[132] concerne sa neutralité à l'égard des outils technologiques, ce qui constituait un avantage par rapport à la *Utah Digital Signature Act*[133]. L'orientation du législateur de l'Utah pouvait être susceptible de freiner le développement et l'acceptation par le législateur de technologies alternatives.

Une autre lacune juridique importante a trait au manque d'uniformité entre les lois canadiennes ainsi qu'à l'échelle internationale. Les lois des provinces canadiennes anglaises n'abordent pas les techniques de cryptographie, se contentant d'admettre les signatures électroniques. Malgré quelques faiblesses, la loi québécoise est généralement bien perçue au Canada anglais, mais il ne semble pas que cette perception ait motivé les législateurs canadiens anglais à prendre cette direction. Cette inégalité de traitement est susceptible d'engendrer une incertitude pour les usagers et, surtout, pour les consommateurs.

Le volet technique de la sécurité est également perfectible. Le protocole de communication sécurisé SSL connaît ses limites. Les fraudeurs sont sensibilisés au fait que les usagers d'Internet apportent une plus grande attention à la sécurité. Par conséquent, les sites miroirs bancaires ou de paiement utilisés par des fraudeurs sont désormais sécurisés par SSL et le certificat joint se présente comme appartenant au site véritable[134]. La chaîne de certification y est par contre forgée. Il est donc plus difficile pour l'usager de détecter la fraude sans consulter la chaîne de certification et découvrir qu'une autorité supérieure de la chaîne n'a pas réellement certifié le site pirate. L'internaute se heurte également à des difficultés de consultation des critères de labellisation, ce qui peut le conduire à croire à une fausse sécurité. Tel pourrait être le cas, par exemple, si le label garantit la protection de la vie privée, mais non la confidentialité et la sécurité du site. De plus, la labellisation étant généra-

---

132 Précitée, note 1.

133 Voir *supra*, notes 56-58 et le texte correspondant.

134 Nick FARRELL, « PayPal Fixes Fatal Flaw », *The Inquirer* (19 juin 2006), en ligne : [http://www.theinquirer.net/?article=32493].

lement coûteuse, elle est peu accessible aux sites transactionnels de moindre envergure. Ensuite, le processus de certification croisée est habituellement imposé par les autorités de certification. Pour diverses raisons – accès difficile, documents trop volumineux et techniques, notamment –, l'usager ne consulte que très rarement les certificats et les énoncés de politique. Toutefois, l'usager qui se réfère à un certificat de l'autorité cocertifiée par sa propre autorité de certification, mais qui ne reçoit aucune alerte de sécurité, ne peut savoir qu'il fait affaire avec un autre tiers certificateur dont il ne connaît pas les politiques. De plus, il faut constater une absence d'autorité racine et une concentration élevée de certificats à l'échelle mondiale émis par un faible nombre d'autorités de certification privées – Verisign, Identrust. Enfin, bien que respectées d'un point de vue pratique, les normes ISO et UIT ne sont pas contraignantes.

II. Le développement des modèles de certification supérieure

Comme nous venons de le constater, les initiatives juridiques et techniques mises en place afin d'assurer une plus grande sécurité des transactions bancaires en ligne n'offrent pas de solutions parfaites, mais elles constituent un pas dans la bonne direction. Le manque d'encadrement juridique des activités des autorités de certification laisse planer un doute sur le degré réel de sécurité offert. Afin d'offrir un environnement de confiance aux usagers dans Internet, il est nécessaire d'implanter des mécanismes de supervision des autorités de certification (A) et de définir clairement la responsabilité des certificateurs et des banques utilisant leurs services (B).

A. Les mécanismes de supervision

Il existe à ce jour quelques mécanismes de supervision des autorités de certification. Certains sont contraignants pour l'autorité de certification alors que d'autres imposent à l'usager la responsabilité de la supervision. Ce dernier n'est cependant pas suffisamment outillé pour effectuer efficacement cette supervision et, le cas échéant, ordonner des mesures correctives à l'autorité de certification. Le mécanisme de supervision idéal consiste en une hiérarchie d'autorités de certification indépendantes où chaque autorité de certification supérieure certifie et supervise les autorités de certification

subalternes[135]. Dans les faits, la forme de supervision la plus répandue dans le milieu des transactions bancaires et du commerce électronique est l'autosupervision (1) alors que le milieu des communications administratives et interentreprises fait plus facilement appel à une supervision indépendante de niveau supérieur (2). Nous examinons maintenant ces divers mécanismes de supervision.

1. L'autosupervision

À ce jour, les banques hésitent à se positionner comme autorité de certification pour leur clientèle et préfèrent traiter avec des autorités de certification indépendantes pour assurer le service sécurisé de leurs activités en ligne[136]. Le protocole de sécurité couramment utilisé pour les activités bancaires en ligne est le SSL[137]. Ce protocole permet divers niveaux de sécurité qui concernent le chiffrement de communications de même que l'octroi et la vérification de certificats numériques. Le niveau utilisé pour les services bancaires en ligne nécessite la délivrance d'un certificat pour le serveur de l'établissement financier, mais il n'est pas nécessaire pour le client, puisqu'il est reconnu simplement par son identifiant et par son mot de passe[138].

De manière simplifiée, une communication protégée par SSL débute par un dialogue entre le serveur de la banque et le terminal du client. Lorsque le certificat du serveur est reconnu par le terminal du client, une paire de clés numériques est attribuée à la session sécurisée demandée[139]. Pour ces étapes d'ouverture d'une session en ligne, le client n'a aucun geste à poser, le processus étant entiè-

---

135 A.M. FROOMKIN, *loc. cit.*, note 13, 56.

136 Tara C. HOGAN, « Now that the Floodgates Have Been Opened, Why Haven't Banks Rushed Into the Certification Authority Business? », 4 *N.C. Banking Inst.* 417, 430 (2000).

137 *Supra*, section I.B.2.A.

138 Ceux-ci constituent une signature au sens du droit québécois et canadien : art. 2827 C.c.Q. ; *Loi sur la protection des renseignements personnels et les documents électroniques*, précitée, note 38, art. 31(1). Ce type d'identification est acceptable dans une transaction virtuelle impliquant des parties ayant une connaissance préalable l'une de l'autre (la banque et son client) : D. Scott ANDERSON, « What Trust is in These Times? Examining the Foundation of Online Trust », *54 Emory L.J.* 1441, 1462 (2005).

139 T. ONYSZKO, *loc. cit.*, note 63, 5.

rement transparent[140]. Après l'ouverture de la session et l'établissement de la communication entre le serveur et le terminal du client, une icône apparaît sur le navigateur (interface) du client pour indiquer que la session est sécurisée[141].

Les cas d'autosupervision que nous abordons dans les sous-sections suivantes supposent la négociation d'une communication protégée par SSL. D'abord, nous traitons de l'autosupervision où n'intervient qu'un seul palier de certification (a). Ensuite, nous portons notre attention sur l'autosupervision pyramidale qui met en jeu plusieurs paliers d'une autorité de certification unique (b). Enfin, nous examinons les hiérarchies de certification trompeuses (c).

a. L'autocertification

Comme son nom l'indique, l'autocertification suppose l'intervention d'un seul palier de certification. L'autorité de certification émet elle-même son propre certificat et le déclare valide[142]. Cette autocertification peut provenir d'un serveur marchand ayant créé sa propre infrastructure à clé publique pour sa clientèle[143] ou de l'autorité racine d'une chaîne de certification[144]. Dans la plupart des cas, les certificats sont délivrés pour une période de plusieurs années sans le bénéfice des vérifications indépendantes annuelles offertes par la labellisation[145]. Il apparaît clairement que la princi-

---

140 Les usagers qui utilisent la cryptographie à clé publique tel SSL n'ont habituellement pas connaissance de la complexité du processus de chiffrement : D.S. ANDERSON, *loc. cit.*, note 138, 1455 ; THAWTE, « Sécurisez des transferts de données en ligne avec SSL », Cape Town (South Africa), Thawte, 2005, p. 9, en ligne : [http://www.thawte.com/ssl-digital-certificates/free-guides-whitepapers/pdf/ssl_fr.pdf].

141 *Supra*, note 67.

142 A.M. FROOMKIN, *loc. cit.*, note 13, 56-58.

143 Dans un tel cas, le serveur marchant accorde plus d'importance au cryptage de la communication qu'à la vérification de l'identité du cocontractant. Voir à ce sujet le site de Les Technologies DeltaCrypt : [http://www.deltacrypt.com/francais/home/index.html]. Voir également le tutoriel permettant de créer sa propre infrastructure à clé publique : Timothy BORONCZYK, « Generating Your Own Security Certificates For Use With Apache/HTTPS », Codewalkers, Syracuse, 2004, en ligne : [http://codewalkers.com/tutorialpdfs/tutorial59.pdf].

144 À titre d'exemple, le certificat racine de l'autorité de certification Verisign.

145 *Supra*, section I.B.2.b. La racine de Verisign est valide jusqu'en 2028 et le second palier jusqu'en 2011. Froomkin abordait la durée de validité des certificats sous l'angle d'une fiabilité accrue par une durée limitée, obligeant la réémission

pale lacune liée à ce type de certification provient de l'absence de supervision extérieure. Malgré une lecture attentive de la politique de certification de l'autorité, l'usager ne possède aucun moyen concret de vérifier si les représentations qui lui sont faites sont réellement appliquées. Comme le souligne un auteur : « [i]*t is one thing to trust the credentials within the eloquently secure architecture of PKI ; it is entirely different to trust that the* [certification authorities] *has properly granted those credentials allowing access to the network of trust* »[146].

Plusieurs de ces autorités de certification à un seul niveau sont des entreprises privées ou sans but lucratif[147]. Elles opèrent de façon restreinte et souvent dans un secteur particulier[148]. Elles ne font pas partie des autorités de certification reconnues par les navigateurs Internet et l'usager qui accède à un site sécurisé par ces autorités de certification reçoit un message d'alerte qui indique que l'autorité de certification n'est pas reconnue par son ordinateur. L'usager peut alors décider de continuer la transaction sans se préoccuper de l'alerte. Le cas échéant, il accède à une communication sécurisée par une autorité de certification inconnue et il engage alors sa propre responsabilité[149].

L'usager peut aussi décider de vérifier les engagements et la crédibilité de l'autorité de certification en consultant ses certificats[150]. Il devra ensuite prendre connaissance de la politique de certification

---

régulière de ces derniers. Il semble que ce ne soit pas la solution adoptée par les autorités de certification actuelles : A.M. FROOMKIN, *loc. cit.*, note 13, 61.

146 D.S. ANDERSON, *loc. cit.*, note 138, 1463.

147 Pour un organisme sans but lucratif, voir le site de Selso : [http://www.selso.com].

148 Voir à ce sujet l'infrastructure à clé publique du Centre National de la Recherche Scientifique (ci-après cité « CNRS ») : CNRS, « Autorité de Certification CNRS-Standard », en ligne : [http://igc.services.cnrs.fr/CNRS-Standard].

149 *Loi concernant le cadre juridique des technologies de l'information*, précitée, note 1, art. 62. La connexion étant sécurisée par SSL, les données échangées entre le client et le site Internet ne peuvent être interceptées en cours de route. Cependant, le client n'a pas reçu confirmation de l'identité du site Web et n'a donc pas la certitude de communiquer avec l'entité souhaitée.

150 *Id.*, art. 60. Celui qui entend se fier à un certificat doit en vérifier la validité et la véracité.

de cette autorité avant de décider s'il lui accorde sa confiance[151] et ainsi installer le certificat racine sur son ordinateur[152]. Par la suite, tous les certificats émis par cette autorité de certification seront reconnus par le navigateur et aucune alerte de sécurité ne sera affichée de nouveau.

Ce type de certification fait reposer le processus de supervision et de décision sur les épaules de l'usager[153] alors que l'autorité de certification s'appuie uniquement sur sa réputation. La notion de tiers certificateur indépendant, fondamentale en matière de certification Internet, est également absente en l'espèce[154].

---

151 L'article 52 de la *Loi concernant le cadre juridique des technologies de l'information*, précitée, note 1, donne l'information minimum devant être contenue dans un énoncé de politique. Cet énoncé contient en moyenne une quarantaine de pages et plusieurs termes techniques. L'article 52, al. 2 *in fine* de cette loi précise que cet énoncé doit être accessible au public. Dans les faits, bien que l'adresse à laquelle il est possible de consulter cet énoncé figure au certificat, il est extrêmement difficile de la repérer.

152 Plusieurs autorités de certification ont conclu des ententes avec les principaux navigateurs Internet afin que leurs certificats racines y soient installés par défaut. Le logiciel d'exploitation Windows XP contient 107 certificats racines pré-installés provenant de 22 autorités de certification. Lorsqu'un certificat racine est installé par défaut, le terminal de l'usager le reconnaît et n'affiche aucune alerte de sécurité. Le seul indice que ce dernier vient d'entrer en communication sécurisée est l'apparition de l'icône de sécurité dans le bas de l'écran. Lorsqu'un usager doit franchir les étapes d'installation d'un certificat racine, il acquiert une certaine connaissance des engagements pris par l'autorité de certification envers les utilisateurs qui acceptent de faire confiance à ses certificats. Lorsque le certificat racine d'une autorité de certification est pré-installé dans le navigateur Internet, l'usager ne se voit pas réellement offrir le choix de faire confiance ou non à cette autorité de certification. Cette transparence face à tous les certificats racine pré-installés rend plus difficile l'éducation des consommateurs puisqu'il faut d'abord les sensibiliser à une pratique dont ils ne sont pas conscients. Voir : Jane K. WINN, « The Emperor's New Clothes: The Shocking Truth About Digital Signatures and Internet Commerce », 37 *Idaho L. Rev.* 353, 376 (2001).

153 A.M. FROOMKIN, *loc. cit.*, note 13, 61 ; *Loi concernant le cadre juridique des technologies de l'information*, précitée, note 1, art. 61. L'obligation de vérification qui incombe au consommateur est une obligation de moyens. Cependant, compte tenu de l'utilisation abondante de termes techniques dans les énoncés de politiques, nous ne croyons pas que l'obligation de moyens implique pour le consommateur des recherches supplémentaires afin de se familiariser avec ces termes. Il en résulte que malgré une lecture attentive, ce langage hermétique n'apportera pas au consommateur le degré de compréhension désiré.

154 *Loi concernant le cadre juridique des technologies de l'information*, précitée, note 1, art. 56 ; T.C. HOGAN, *loc. cit.*, note 136, 425 ; D.S. ANDERSON, *loc. cit.*, note 138, 1458.

b. L'autocertification pyramidale

Dans cette forme de hiérarchie, tous les paliers de certification sont certifiés par la même autorité de certification. La différence de sécurité entre les différents paliers provient du type de contrôle et de vérification que l'autorité de certification s'engage à offrir. Plus le palier est élevé, plus les critères à rencontrer pour se voir émettre un certificat sont élevés[155]. Au Québec, pour être considéré comme un palier distinct, chaque palier de certification de l'autorité unique doit offrir des garanties d'indépendance suffisantes dans le but de satisfaire aux conditions d'impartialité prévues par la loi[156].

Dans le cas d'une autocertification pyramidale, l'usager croit se trouver en présence d'une autorité de certification elle-même certifiée par une autorité de certification supérieure. Il peut conclure que l'environnement Internet où il se trouve est plus sécuritaire que lors d'une certification à un seul palier. Pourtant, le seul moyen de juger du degré de sécurité offert à chaque palier consiste à prendre connaissance de la politique de certification de l'autorité de certification afin de déterminer les exigences de sécurité, de vérification et d'identification auxquelles chaque palier doit répondre avant l'émission du certificat[157]. Ainsi, la simple présence d'une certification pyramidale n'est pas garante d'une sécurité supérieure si, dans les faits, les divers paliers supérieurs sont soumis à des exigences moins strictes qu'une autorité de certification à un seul palier très réglementé[158].

Le nombre de paliers de certification n'offre donc pas nécessairement une plus grande sécurité. En l'espèce, le processus de supervision et de décision impose une responsabilité plus importante à l'usager qui doit consulter non seulement l'énoncé de politique de l'autorité de certification directement liée à sa transaction, mais également l'énoncé de politique des paliers supérieurs avant de déter-

---

155 A.M. FROOMKIN, *loc. cit.*, note 13, 56.

156 *Loi concernant le cadre juridique des technologies de l'information*, précitée, note 1, art. 56.

157 Un certificat qui exige la simple confirmation d'un pseudonyme par courriel constitue un certificat de peu de valeur puisqu'il ne garantit que la validité d'une adresse courriel et non l'identité du détenteur de cette adresse. Voir *supra*, note 147; A.M. FROOMKIN, *loc. cit.*, note 13, 58.

158 D.S. ANDERSON, *loc. cit.*, note 138, 1459.

miner le degré de confiance qu'il entend leur accorder[159]. De plus, encore une fois, la présence du critère d'indépendance peut être mise en doute[160].

c. Les hiérarchies trompeuses

L'internaute est parfois en présence d'une hiérarchie de certification impliquant plus d'une autorité de certification. Au premier coup d'œil, le tiers certificateur indépendant semble présent puisque deux ou plusieurs entités distinctes ont effectué un contrôle préalable à l'émission du certificat consulté. Cette situation est préférable à l'autocertification. Cependant, les autorités de certification racine opérant dans Internet ne sont pas légion[161]. Au fil des ans et des développements, le phénomène de convergence a incité plusieurs autorités de certification à acquérir d'autres autorités de certification moins importantes ou concurrentes[162], ce qui est susceptible de créer des hiérarchies dites de « certification trompeuse » auxquelles se heurte le consommateur.

Dans ces hiérarchies trompeuses, les diverses autorités de certification impliquées portent des noms distincts, mais elles sont liées entre elles. Il peut s'agir d'une filiale à 100 % de l'autorité de certification racine, ou encore d'une même autorité de certification qui utilise des noms de commerce distincts pour les divers paliers de certification qu'elle offre. À titre d'exemple, l'autorité de certification Thawte[163] est elle-même certifiée par l'autorité racine de Verisign. Cependant, l'autorité de certification Thawte est en réalité une filiale

---

159 *Loi concernant le cadre juridique des technologies de l'information*, précitée, note 1, art. 61 ; A.M. FROOMKIN, *loc. cit.*, note 13, 56.

160 *Loi concernant le cadre juridique des technologies de l'information*, précitée, note 1 ; T.C. HOGAN, *loc. cit.*, note 136, 425 ; D.S. ANDERSON, *loc. cit.*, note 138, 1458.

161 Une autorité de certification racine désigne l'autorité de certification qui occupe l'échelon le plus élevé d'une hiérarchie de certification.

162 Depuis 1995, Verisign à acquis 12 autorités de certification et entreprises de développement technologique, signé plusieurs partenariats avec des compagnies tels que Visa, Intel, Microsoft, At&T et Kodak, et est impliquée directement dans le développement de solutions de sécurité Internet de cinq groupes bancaires importants tels que la Sumito Bank (Japon), Morgan Stanley (É.-U.), Barclays (Ang.) et Bank of America (É.-U.). VERISIGN, « Verisign: A History », Verisign, Mountain View (CA), 2005, p. 9, en ligne : [http://www.verisign.com/static/036566.pdf].

163 Voir à ce sujet : [http://www.thawte.com].

détenue à 100 % par Verisign. Au même effet, l'autorité de certification Identrus est certifiée par TrustID, elle-même certifiée par l'autorité racine DigitalTrustService. Lors de la consultation de la chaîne de certification, il n'apparaît pas à l'usager que Identrus est l'ancien nom de l'autorité de certification IdenTrust et que TrustID et DigitalTrustService sont des noms commerciaux qui lui appartiennent.

Ainsi, il n'existe aucune distinction entre les autocertifications pyramidales et les hiérarchies trompeuses, tant sur le plan de l'indépendance du certificateur qu'en ce qui concerne le degré de sécurité lié à chaque palier de certification. Cependant, la difficulté supplémentaire réside dans le fait qu'il est peu probable que l'usager diligent et raisonnable consulte les statuts de constitution de ces autorités de certification afin de déterminer s'il s'agit d'entités liées ou non. Nous ne croyons d'ailleurs pas que ce type de vérification cadre avec l'obligation de moyen qui incombe à l'usager[164]. Cette forme de hiérarchie peut engendrer une confiance accrue de la part des internautes, bien que l'indépendance des autorités de certification les unes envers les autres ne soit pas expressément garantie par une dénomination sociale distincte.

2. La supervision indépendante

Au Canada, peu de banques opèrent une autorité de certification[165]. Ainsi, en regard des banques, les autorités de certification qui sécurisent leur site de transactions bancaires sont indépendantes des banques qu'elles certifient[166]. Par contre, nous avons vu que ces autorités de certification sont engagées dans des hiérarchies d'autocertification ou de certification trompeuse. La chaîne d'indépendance ne subsiste pas au-delà du premier échelon. De plus, l'autorité de certification IdenTrust, détenue par un consortium bancaire, certifie les banques propriétaires, éliminant même ce premier échelon d'indépendance.

---

164 *Loi concernant le cadre juridique des technologies de l'information*, précitée, note 1, art. 61.

165 Seule la Banque Scotia opère présentement une autorité de certification au Canada, en ligne : [http://www.scotiabank.com/cda/content/0,1608,CID6092_LIDfr,00.html].

166 Au Canada, les sites de transactions bancaires en ligne des banques de l'Annexe 1 sont sécurisés par les autorités de certification Verisign, Entrust et Thawte.

Il existe néanmoins quelques autorités de certification indépendantes de niveau supérieur qui oeuvrent dans divers secteurs. Certains États ont légiféré afin d'encadrer les activités des autorités de certification qui opèrent sur leur territoire[167]. Dans cette section, nous abordons d'abord la réalité des autorités de certification supérieures commerciales (a) pour analyser par la suite le cas des autorités de certification gouvernementales (b). Notre attention se porte ensuite sur l'encadrement offert par diverses législations étatiques (c), puis nous terminons en soulignant les obstacles à la création d'une chaîne de certification indépendante idéale (d).

a. Les autorités de certification supérieures « commerciales »

En 1999, l'Eurochambres[168] et l'Association des Chambres européennes de commerce et d'industrie ont fondé l'autorité de certification Chambersign[169], laquelle représente une autorité racine destinée aux chambres de commerce et d'industrie des États européens et au commerce électronique en général[170]. Chambersign a pour mission de créer un environnement sécurisé pour le commerce électronique local et outre frontière[171]. Aujourd'hui, Chambersign Europe regroupe les réseaux de chambres de commerce et d'industrie de dix États membres[172]. Les certificats et signatures émis par n'importe laquelle des chambres de commerce locales ou nationales sont reconnus sur l'ensemble du territoire couvert par Chambersign Europe[173]. L'initiative des chambres de commerce européennes rejoint sensiblement l'idée d'une chaîne de certification idéale. L'organisme supranational Eurochambres agit à titre d'autorité de certification racine alors que les organismes nationaux – les associations des chambres de commerce et d'industrie des dix États membres –

---

167 En Amérique du Nord, l'Utah a été le premier État des États-Unis à encadrer les activités des autorités de certifications : *supra*, note 56 et texte correspondant.

168 Voir à ce sujet le site d'Eurochambres : [http://www.eurochambres.be].

169 Voir à ce sujet le site de ChamberSign : [http://www.chambersign.com].

170 La clientèle visée dès sa création comprenait 579 chambres de commerce locales et plus de 13 millions d'entreprises. Voir : CHAMBERSIGN, « About Us », en ligne : [http://www.chambersign.com/aboutus.htm].

171 *Id.*

172 L'Allemagne, l'Autriche, la Belgique, l'Espagne, la France, la Grande-Bretagne, l'Italie, le Luxembourg, les Pays-Bas et la Suède.

173 Voir le site Web : [http://www.chambersign.tm.fr/chambersign/reseau-eu.jsp].

interviennent comme certificateurs subalternes. Les organismes régionaux – les chambres de commerce et d'industrie régionales – interviennent au troisième niveau et les entreprises et les particuliers occupent le niveau inférieur de la chaîne. Chambersign est également membre de la Fédération nationale des tiers de confiance[174].

En France, l'autorité de certification Certinomis[175] est une filiale de La Poste[176]. Elle offre le service de certification racine aux entreprises, aux institutions financières et aux services administratifs. Elle délivre également des certificats aux personnes physiques, tant pour leur propre compte que pour la représentation d'une entreprise. Un grand avantage provient de sa facilité d'accès. En effet, la remises de documents et l'identification en personne nécessaire à l'émission d'un certificat de « catégorie 3 » peuvent être effectuées dans n'importe quel bureau de poste sur le territoire français de même qu'auprès de certaines banques et sociétés de services[177]. En 2004, la banque Odier Bungener Courvoisier[178] a choisi Certinomis pour la certification racine de ses opérations électroniques[179]. Elle est également une autorité de certification reconnue par plusieurs services gouvernementaux[180]. Tout comme Chambersign, Certinomis est membre de la Fédération nationale des tiers de confiance[181].

---

174 Il s'agit d'une organisation professionnelle dont les statuts sont régis par le *Code du Travail* français dont le but premier est d'établir et promouvoir la sécurité et la qualité des prestations de certification dans les nouveaux environnements techniques. Voir le site Web : [http://www.fntc.org].

175 Voir le site Internet : [http://www.certinomis.com].

176 Voir la vitrine Internet : [http://www.laposte.fr].

177 La certification de classe 3 délivrée par Certinomis nécessite une vérification d'identité en face à face préalablement à la délivrance des codes d'activation des certificats. Il s'agit du plus haut niveau de sécurité offert par Certinomis : CERTINOMIS, *Politique de certification – classe 3*, version 1.2, CERTINOMIS, 2002, p. 12, en ligne : [https://www.certinomis.com/publi/pc/pol_3_2.pdf].

178 Filiale du consortium bancaire hollandais ABN AMRO.

179 NOTE, « OBC dématérialise ses flux bancaires avec Certinomis », Communiqué de Presse, Paris, 17 novembre 2004, en ligne : [http://www.certinomis.com/fichiers/guides/CP_OBC%20nov04.pdf].

180 Notamment le MINÉFI et le ministère de la Défense.

181 *Supra*, note 174.

Au Québec, le Centre de certification du Québec joue un rôle de plus en plus actif sur le plan de la sécurité des communications[182]. Développé par Notarius à la suite du succès de l'implantation de l'infrastructure à clé publique de la Chambre des notaires en 1998[183], le Centre de certification du Québec offre des services de certification numérique aux arpenteurs-géomètres, aux évaluateurs agréés, aux technologues professionnels et à la clientèle de la firme SNC Lavalin Inc.[184].

L'infrastructure de certification mise sur pied par Notarius pour les notaires permet à ces derniers d'effectuer plusieurs transactions immobilières sur support électronique par le biais de partenariats avec les Caisses d'épargnes Desjardins et la société BCE Emergis[185]. Pour ces infrastructures, Notarius constitue l'autorité de certification racine qui émet, gère et révoque les certificats numériques et les clés publiques et privées qui y sont liées.

Le Centre de certification du Québec est également cocertifié par le Conseil du trésor, ce qui permet aux détenteurs de ses certificats de transiger avec le Registre foncier du Québec[186]. Les notaires agents vérificateurs d'identité sont mandatés par le ministère de la Justice du Québec afin de vérifier l'identité des demandeurs de

---

182 Voir à ce sujet : NOTARIUS, « Centre de certification du Québec », 2006, en ligne : [http://www.notarius.com/public/ccq/ccq.html]. Notarius est la filiale technologique de la Chambre des notaires du Québec. Voir le site de Notarius : [http://www.notarius.com].

183 L'infrastructure à clé publique de la Chambre des notaires est une part importante de la phase II du plan de développement de Notarius consistant à doter la profession notariale d'un Intranet sécurisé et de signatures numériques permettant aux notaires de chiffrer et signer leurs communications et documents sur support informatique : NOTARIUS, « Profil d'entreprise : Son évolution (phase II) », Montréal, Notarius, 2006, en ligne : [http://www.notarius.com/public/profil/evolution_phase2.html].

184 Il est possible de consulter les ententes et exigences de délivrance et de la gestion des certificats numériques pour chacun de ses ordres professionnels et services gouvernementaux sur le site du centre de certification du Québec : NOTARIUS, « Centre de certification du Québec », 2006, en ligne : [http://www.notarius.com/public/ccq/ccq.html].

185 Cette innovation a pris place pendant la phase III du développement de Notarius : NOTARIUS, « Profil d'entreprise. Son évolution (phase III) », Montréal, Notarius, 2006, en ligne : [http://www.notarius.com/public/profil/evolution_phase3.html] ; NOTARIUS, « Qui fait quoi et à quelle fin ? », Montréal, Notarius, 2004, 10, en ligne : [http://www.notarius.com/doc/p0078_BrNotariusCor.pdf].

186 NOTARIUS, « Qui fait quoi et à quelle fin ? », *id.*, 6.

certificats numériques pour l'infrastructure à clé publique du gouvernement du Québec[187]. Les notaires agents vérificateurs d'identité vérifient également les demandes de certificats en vue de transiger avec la Société d'assurance automobile du Québec et le Registre des lobbyistes[188], deux autorités de certification de second niveau qui relèvent de l'infrastructure gouvernementale, de même que pour la clientèle de l'infrastructure à clé publique du Registre des droits personnels et réels mobiliers[189]. Les notaires utilisent la signature numérique et les certificats délivrés par Notarius pour remplir leur rôle d'agents vérificateurs pour ces autorités de certification.

Bien qu'elle soit une filiale de la Chambre des notaires, Notarius respecte le degré d'impartialité requis par la loi[190]. En tant qu'autorité racine des infrastructures à clé publique des ordres professionnels des notaires, des arpenteurs-géomètres, des évaluateurs agréés et des technologues professionnels, elle assure la supervision de la chaîne de certification qui en découle. Les infrastructures mises sur pied par Notarius utilisent le logiciel de signature et de chiffrement *Entrust Intelligence*[191], développé par l'autorité de certification Entrust. Cette dernière n'intervient toutefois pas dans les chaînes de certification de Notarius.

b. Les autorités de certification gouvernementales

Les initiatives des gouvernements en ligne sont nombreuses[192]. Ainsi, il existe plusieurs autorités de certification gouvernementales de niveau supérieur. Principalement destinées à assurer une chaîne de certification dans un domaine précis de la fonction publique, elles fonctionnent en vase clos et elles sont rarement destinées

---

187 *Id.*

188 *Id.*, 7.

189 Voir le site de Notarius : [http://avi.notarius.net].

190 *Loi concernant le cadre juridique des technologies de l'information*, précitée, note 1, art. 56.

191 Pour plus de détails sur ce logiciel et ses applications, voir en ligne : [http://www.entrust.com/entelligence/index.htm].

192 À titre d'exemple, l'Union européenne et ses États membres travaillent activement à créer un environnement administratif électronique sur l'ensemble du territoire européen. Pour un survol des États impliqués et des initiatives entreprises, voir : EURACTIV.COM, « L'administration en ligne (e-gouvernement) », 18 août 2004, en ligne : [http://www.euractiv.com/fr/societe-information/administration-ligne-gouvernement/article-120291].

à agir comme autorité racine pour des services commerciaux ou pour des services aux particuliers.

Au Canada, l'infrastructure à clé publique du gouvernement fédéral agit à titre d'autorité de certification racine pour la certification des différents ministères et organismes autorisés[193]. L'installation centrale canadienne agit comme un point central qui reconnaît chacune des autorités de certification des ministères et organismes. Grâce à ce point central, les ministères et les organismes peuvent communiquer de façon sécurisée entre eux sans devoir procéder à une cocertification bilatérale avec chaque ministère ou organisme[194]. L'énoncé de politique de l'infrastructure à clé publique du gouvernement du Canada précise notamment qu'elle entend « [p]ermettre et encourager la coopération et la collaboration entre les autorités de certification du gouvernement et, en leur nom, avec d'autres infrastructures publiques à clé publique gouvernementales et autres, tant au Canada qu'à l'étranger »[195]. Cependant, cette certification racine gouvernementale ne s'intéresse pas aux autorités de certification accessibles aux consommateurs même si elle s'engage à élaborer des normes ouvertes pour ces autorités de certification[196].

En France, tel que nous l'avons souligné en matière de certification croisée[197], l'autorité de certification racine du MINÉFI[198] émet des certificats aux serveurs du ministère et aux autorités de certification cocertifiées et reconnues par le MINÉFI aux fins de téléprocédures. Les particuliers qui possèdent des certificats reconnus par le ministère ne peuvent les utiliser que dans des communications

---

193 Les ministères et organismes pouvant transiger avec l'autorité de certification racine du gouvernement sont disponibles en ligne : [http://www.solutions.gc.ca/pki-icp/crosscert/mem/mem_f.asp].

194 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *Instaurer la confiance : Cocertification avec l'infrastructure à clé publique du gouvernement du Canada*, Ottawa, Gouvernement du Canada, 2005, p. 3, en ligne : [http://www.solutions.gc.ca/pki-icp/crosscert/trust-confiance/trust-confiance_f.rtf].

195 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *Politique de gestion de l'Infrastructure à clé publique au gouvernement du Canada*, Ottawa, Gouvernement du Canada, 2004, p. 4, art. 5 (4), en ligne : [http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/PKI/dwnld/pki_f.rtf].

196 *Id.*, p. 4, art. 5 (5).

197 *Supra*, section I.B.2.c.

198 MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE L'INDUSTRIE, « Délégation aux systèmes d'information – Agence d'autorité », en ligne : [http://www.minefi.gouv.fr/dematerialisation_icp/SITE_AC.htm].

avec ce dernier. Ainsi, tout comme au Canada, ce type de certification illustre comment une autorité gouvernementale peut exercer une supervision indépendante de niveau supérieur dans une hiérarchie de certification. Cependant, l'autorité gouvernementale n'agit pas comme autorité racine pour des autorités de certification commerciales accessibles aux consommateurs.

Ce survol démontre que la technologie de cryptographie asymétrique est reconnue et appliquée par les gouvernements et qu'il ne reste qu'un pas à franchir pour qu'une autorité de certification qui offre ses services aux institutions financières soit certifiée au niveau gouvernemental. À titre d'hypothèse, au Canada, une autorité de certification comme Verisign pourrait être certifiée et supervisée par l'autorité de certification du ministère des Finances, elle-même certifiée par l'autorité racine gouvernementale à la suite de la rencontre de critères prédéterminés[199]. Comme il est possible de déterminer dans un certificat le champ d'utilisation pour lequel il est émis[200], ce certificat s'appliquerait uniquement aux services de chiffrement et de signature des activités bancaires en ligne, limitant d'autant le travail de supervision exigé du ministère.

c. La demande de licence volontaire

Plusieurs États ayant légiféré sur les signatures électroniques, la cryptographie prévoient un mécanisme d'enregistrement auprès d'un organisme mandaté afin de bénéficier de certaines protections et de certains privilèges accordés par la loi[201]. L'octroi d'une licence

---

199 D'ailleurs, la certification par une autorité gouvernementale est différente de l'octroi de licence puisqu'en matière de licence, aucune autorité gouvernementale n'agit comme autorité de certification racine ou supérieure. Une hiérarchie de certification débutant par une certification racine gouvernementale représentait la solution idéale pour Froomkin : A.M. FROOMKIN, *loc. cit.*, note 13, 56.

200 UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS, précitée, note 124. La loi québécoise précise un contenu minimum pour un certificat ; en ce sens, elle exige moins d'informations que la norme internationale n'en contient : *Loi concernant le cadre juridique des technologies de l'information*, précitée, note 1, art. 48.

201 Principalement, les certificats émanant d'une autorité de certification licenciée bénéficient d'une présomption de validité : *Loi concernant le cadre juridique des technologies de l'information*, précitée, note 1, art. 53, al. 2 ; *Utah Digital Signature Act*, précitée, note 56, art. 46-3-401 ; *Décret 2001-273 du 30 mars 2001 pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique*, (2001) J.O. R. F. n° 77/5070, art. 6 et 7 [ci-après cité : « Décret 2001-273 »].

peut également être un atout promotionnel pour l'autorité de certification licenciée[202]. L'organisme accordant la licence procède à une évaluation de l'autorité de certification et de sa politique de certification afin de s'assurer qu'elle se conforme à toutes les dispositions de la loi applicable sur le territoire pour lequel la licence est octroyée. En ce sens, nous considérons cet organisme comme un organisme de supervision. Son champ d'action est cependant limité puisqu'il ne supervise que les autorités de certification qui font une demande de licence.

Aux États-Unis, l'Utah a été le premier État à légiférer sur la signature électronique et à prévoir un mécanisme de licence volontaire pour les autorités de certification[203]. En vigueur de 1995 à 2006[204], cette loi précisait que l'absence de licence ne rendait pas inutilisables les certificats émis par l'autorité de certification, mais prévoyait un traitement préférentiel aux autorités de certification licenciées[205]. En effet, les signatures numériques et les certificats délivrés par une autorité de certification licenciée faisaient l'objet d'une présomption de validité[206]. De plus, l'autorité licenciée bénéficiait d'une limite de responsabilité en regard des dommages-intérêts découlant d'une transaction qui concernait ses certificats[207] et d'une exonération de responsabilité pour usage de faux, fausses représentations ou erreur en regard de ses certificats[208]. Les devoirs et les obligations de l'autorité de certification licenciée figuraient à la troisième partie de la loi, laquelle était toutefois silencieuse sur les devoirs et obligations des autorités de certification non licenciées[209].

---

202 À titre d'exemple, l'autorité de certification Verisign annonce les licences qu'elle détient sur son site Internet : VERISIGN, « Certification Authority and Approvals », 1er décembre 2003, en ligne : [https://www.verisign.com/repository/licenses.html].

203 *Utah Digital Signature Act*, précitée, note 56.

204 Voir *supra*, note 56-58, et le texte correspondant.

205 *Utah Digital Signature Act*, précitée, note 56, art. 46-3-201(5)(a) et (b).

206 *Id.*, art. 46-3-401.

207 *Id.*, art. 46-3-308 (1).

208 *Id.*, art. 46-3-308 (2).

209 *Id.*, titre 3 (art. 46-3-301 à 46-3-309) ; A.M. FROOMKIN, *loc. cit.*, note 13, 50.

Peu d'autorités de certification ont été licenciées en Utah sous cette loi[210].

L'Union européenne prévoit également un processus d'accréditation volontaire des autorités de certifications dans la Directive 1999/93/CE[211]. Chaque État membre doit établir ses critères d'accréditation et les transmettre à la commission[212]. C'est donc dans le corpus juridique interne de chaque État que les autorités de certification trouveront les conditions d'admissibilité et les avantages d'être accrédités[213]. Au Luxembourg, une autorité de certification gouvernementale a été créée à la suite de l'adoption de la Loi du 14 août 2000[214] et prévoit l'accréditation volontaire de prestataires de services de certification[215]. La loi définit le prestataire de service de certification comme « toute personne, physique ou morale, qui délivre et gère des certificats ou fournit d'autres services liés aux signatures électroniques »[216]. Cependant, entre 2000 et 2006, aucun prestataire de service de certification n'a fait de demande d'accréditation[217]. Cette situation peut s'expliquer par une méconnaissance de la part des consommateurs des services de certification, réduisant le besoin pour une autorité de certification de faire une demande d'accréditation auprès d'une autorité supérieure. En effet, l'accréditation suppose des coûts que l'autorité de certification devrait

---

210 Seules les autorités de certification licenciées bénéficiaient des dispositions de la loi. Les autorités de certification non licenciées n'étaient pas soumises à la loi, mais elles pouvaient exercer sur le territoire de l'Utah. Leur situation juridique était aussi incertaine qu'en l'absence de loi. Les entreprises licenciées sous cette loi étaient IdenTrust, UserTrust et Verisign. Pour plus de détails, voir : UTAH, *Division of Corporation and Commercial Code*, 2004, en ligne: [http://www.commerce.utah.gov/corporat/dsmain.htm].

211 *Directive 1999/93/CE*, précitée, note 33.

212 *Id.*, art. 11.

213 Ainsi, en France, ces informations et conditions figurent aux articles 6 et 7 du Décret 2001-273, précité, note 201.

214 *Loi du 14 août 2000 relative au commerce électronique modifiant le code civil, le nouveau code de procédure civile, le code de commerce, le code pénal et transposant la directive 1999/93 relative à un cadre communautaire pour les signatures électroniques, la directive relative à certains aspects juridiques des services de la société de l'information, certaines dispositions de la directive 97/7/CEE concernant la vente à distance des biens et des services autres que les services financiers*, (2000) J.O. G.D.L. A96/2176.

215 *Id.*, art. 30.

216 *Id.*, art. 1.

217 Voir le site Web : [http://www.olas.public.lu/registre/psc/index.html].

refléter dans ses propres tarifs, devenant ainsi moins compétitive sur le marché national.

Au Québec, l'article 53 de la *Loi concernant le cadre juridique des technologies de l'information*[218] prévoit également un régime d'accréditation volontaire. En vertu de l'article 69(3), il appartient au gouvernement de définir les critères et la procédure d'accréditation en adoptant un règlement à cet égard. Depuis l'entrée en vigueur de cette loi en 2001, aucun règlement n'a été adopté en ce sens. À l'instar du Luxembourg, cela illustre un besoin faible, voire inexistant, dans le marché actuel de la certification.

d. Les obstacles à la supervision hiérarchique

Pour ce qui est du volet technique, l'autosupervision et la supervision indépendante ne semblent pas offrir de solutions idéales à la sécurité des sites bancaires en ligne. Les infrastructures nécessaires au développement de hiérarchies de certification pyramidale et à la reconnaissance étatique des autorités de certification sont en place, certes, mais après une croissance fulgurante de la cryptographie, nous assistons à une période de ralentissement dans le développement des solutions de cryptographie en ligne.

Cela peut s'expliquer par l'absence de demande par les usagers. L'utilisation abondante du protocole de chiffrement SSL rend moins nécessaire la distribution de certificats et clés numériques aux particuliers, puisque ces derniers peuvent contracter occasionnellement avec les sites commerciaux de façon sécuritaire sans supporter les coûts d'obtention de signature et de certificats numériques[219]. De plus, les sites transactionnels ne sont pas outillés pour reconnaître et accepter les certificats qui proviennent de plusieurs autorités de certification. À titre d'exemple, un site qui accepte les certificats de l'autorité de certification Verisign ne pourrait transiger qu'avec les clients de Verisign. L'usager qui désire faire affaire avec ce site devrait se procurer un certificat Verisign et en assumer les coûts. S'il désire ensuite négocier avec un autre site qui accepte les certificats

---

218 Précitée, note 1.

219 *Supra,* note 96, et texte correspondant. Le SSL permet au consommateur d'identifier le site Internet avec lequel il transige et assure le chiffrement de la transaction, mais n'offre pas le degré d'identification et de confiance lié à la signature numérique et aux certificats qui l'accompagnent.

émis par IdenTrust, il devra également se procurer les certificats requis à ses frais.

En ce qui a trait aux sites bancaires en ligne, la banque et le client ont déjà établi une relation de confiance rendant moins nécessaire la présentation de certificats d'identification[220], car la banque possède déjà les pièces d'identité et les informations personnelles du client dans son dossier et le client a déjà choisi son institution financière lors de l'ouverture de son compte[221]. Dans la majorité des cas, il est impossible d'ouvrir un compte bancaire en ligne sans se présenter en personne à une succursale de l'institution financière. Cette situation est préférable à une ouverture de compte en ligne qui présente un danger plus important tant pour le consommateur que pour la banque.

En ce qui concerne le volet juridique, les lacunes législatives, tant pour ce qui est de l'absence de lois que du faible pouvoir coercitif des lois existantes, peuvent expliquer en partie les obstacles au développement d'une hiérarchie de certification indépendante idéale. À titre d'exemple, la *Loi concernant le cadre juridique des technologies de l'information* prévoit la création d'un comité chargé d'œuvrer au plan national et international à l'harmonisation des procédés, normes et standards techniques en collaboration avec le Bureau de normalisation du Québec[222]. Ce comité a pour but d'élaborer des guides de pratiques à l'usage des intervenants dans les domaines touchés par la loi[223]. À ce jour, aucun guide de pratique n'a été produit et publié au Bureau de normalisation du Québec[224].

B. La responsabilité

L'état actuel du droit bancaire canadien autorise les banques à exploiter des entités qui offrent des services de certification, que ce soit au niveau subalterne ou supérieur. Il serait intéressant que les chambres de compensation et les associations bancaires professionnelles agissent à titre d'autorités de certification de niveau supérieur.

---

220 D.S. ANDERSON, *loc. cit.*, note 138, 1462.

221 N. L'HEUREUX, É. FORTIN et M. LACOURSIÈRE, *op. cit.*, note 8, nº 1.25(b), p. 97-99.

222 Précitée, note 1, art. 63.

223 *Id.*, art. 65.

224 *Id.*, art. 65, al. 3.

Cette structure n'accorde une certaine sécurité à l'usager que s'il peut tenir la banque et/ou l'autorité de certification responsable d'une erreur. Le cas échéant, quels sont les recours juridiques de l'usager contre la banque ?

Depuis plusieurs années, les services bancaires ont été informatisés d'une manière qui pourrait être qualifiée d'unilatérale, c'est-à-dire que la banque a, en quelque sorte, imposé son système informatique à sa clientèle. Cette situation n'est pas à dénigrer *per se*, puisque les usages bancaires imposent à la banque l'obligation de se tenir à jour dans le développement de ses activités et ceci est bénéfique pour les clients. Dans ce contexte, Luc Thévenoz opine : « *From a loss-avoidance viewpoint, the banks who design, operate, and supervise the system are in the best position to make the optimal decision about the efficient level of precautions at which the marginal cost of any improvement exceeds the marginal gain in reduced losses* »[225]. Une revue de la législation de plusieurs États, dont les États-Unis, le Royaume-Uni, le Danemark, l'Australie et la Nouvelle-Zélande, confirme ce point de vue[226]. En droit bancaire canadien, les banques sont soumises à une obligation générale de prudence et de diligence dans l'exécution de leurs fonctions, ce qui pourrait inclure, selon nous, les activités de certification[227].

Peut-on conclure qu'une erreur commise par une autorité de certification engendre automatiquement la responsabilité de la banque ? Une étude de la responsabilité des autorités de certification est nécessaire (1) avant d'entreprendre l'analyse de la responsabilité de la banque en fonction de la qualification juridique de sa relation avec l'autorité de certification (2). Nous examinons par la suite les possibilités pour la banque de s'exonérer de ses obligations (3).

---

225 Luc THÉVENOZ, *Error and Fraud in Wholesale Funds Transfers: U.C.C. Article 4A and the UNCITRAL Harmonization Process*, Zürich, Schulthess Polygraphisher Verlag, 1990, p. 50.

226 Benjamin GEVA, « Consumer Liability in Unauthorized Electronic Funds Transfers », (2003) 38 *Can. Bus. L.J.* 207, 241-267 ; N. L'HEUREUX, É. FORTIN et M. LACOURSIÈRE, *op. cit.*, note 8, n° 1.182, p. 373-380.

227 N. L'HEUREUX, É. FORTIN et M. LACOURSIÈRE, *op. cit.*, note 8, p. 372.

1. La responsabilité de l'autorité de certification

Nous avons expliqué plus haut que la *Loi concernant le cadre juridique des technologies de l'information*[228] prévoit les droits et les obligations des parties lorsqu'une autorité de certification, appelée prestataire de services dans la loi, prend part à une transaction électronique[229]. En général, les obligations des autorités de certification concernent la gestion des certificats – y compris l'énoncé de politique – et du répertoire[230]. Ces obligations s'adressent aux autorités de certification de niveaux subalterne et supérieur, puisque les autorités de certification de niveau supérieur émettent des certificats aux subalternes.

La délivrance ou le renouvellement du certificat doit comprendre, en outre, le nom distinctif du prestataire de services, la version et le numéro de série du certificat, la période de validité[231] et la référence à l'énoncé de politique[232]. La loi exige également l'obligation pour les prestataires de services de tenir compte de l'identité de la personne qui fait la demande, de l'étendue de l'expertise, de l'infrastructure mise en place, des services offerts ainsi que de la régularité et de l'étendue des audits effectués, de la disponibilité de garanties financières pour exercer l'activité, des garanties offertes quant à l'indépendance et à l'intégrité du prestataire de services, des garanties d'accessibilité et de sécurité des certificats ou des répertoires ainsi que de l'applicabilité des politiques énoncées[233].

Les obligations d'impartialité du prestataire, tant à l'égard du titulaire que d'un tiers, et d'intégrité du certificat, sont prévues à l'article 56 de la loi. L'article 56 *in fine* oblige le prestataire de services à vérifier l'information transmise lors de la délivrance d'un certificat, car une absence ou une insuffisance de vérification constitue une fausse représentation. De plus, le prestataire de services

---

228 Précitée, note 1.

229 Aux fins de la présente discussion, nous ne traiterons que de la responsabilité de l'autorité de certification.

230 Il est destiné à identifier une personne ou un objet, ou même à établir une connexion entre les deux : *Loi concernant le cadre juridique des technologies de l'information*, précitée, note 1, art. 50, al. 1.

231 *Id.*, art. 48, al. 2.

232 *Id.*, art. 48, al. 2 (2) et art. 52, al. 1. L'énoncé de politique doit être accessible au public : *id.*, art. 52, al. 2.

233 *Id.*, art. 55.

doit préserver la confidentialité des secrets commerciaux[234]. Cela représente une obligation cruciale lorsque l'autorité de certification est liée de manière corporative ou contractuelle à la banque. Bien qu'en apparence, une banque qui offre des services d'autorité de certification à ses clients ne soit pas un tiers, et donc ne semble pas présenter *prima facie* des garanties d'impartialité, une structure hiérarchique permet de combler cette lacune.

Enfin, l'article 61(2) prévoit que les prestataires de services de certification et de répertoire « ne sont tenus qu'à des obligations de moyens »[235], et ils ne peuvent refuser d'assumer leur part de responsabilité qui émane de « l'inexactitude ou de l'invalidité du certificat, ou d'un renseignement contenu au répertoire ». La *Loi concernant le cadre juridique des technologies de l'information*[236] n'étant pas d'ordre public, le prestataire de services de certification peut déroger conventionnellement aux articles 56 et 57[237].

2. La responsabilité de la banque dans sa relation avec l'autorité de certification

En regard des services de certification, la responsabilité de la banque dépend de la relation juridique entre celle-ci et l'autorité de certification. La banque peut opérer une autorité de certification selon diverses structures, soit en vertu de la *Loi sur les banques* ou en vertu de certaines institutions du droit civil, comme le mandat et le contrat d'entreprise ou de service[238]. La banque peut également n'avoir qu'un lien indirect avec l'autorité de certification. Nous analysons ces cas de figure dans les paragraphes qui suivent.

Premièrement, la *Loi sur les banques* permet aux banques à charte canadiennes d'exploiter des services d'autorité de certification depuis 1997[239]. En vertu de l'article 468(2)(a), une banque a maintenant le droit d'« acquérir ou [d']augmenter un intérêt de groupe

---

234 *Id.*, art. 57.

235 *Id.*, art. 61.

236 Précitée, note 1.

237 Il n'existe aucune indication dans la loi à savoir que celle-ci est d'ordre public.

238 Aux fins de nos recherches, il fut impossible de consulter ces contrats. Nous nous basons sur des situations hypothétiques.

239 *Loi sur les banques*, L.C. 1991, c. 46, modifiée par la *Loi modifiant la législation relative aux institutions financières*, L.C. 1997, c. 15, art. 42.

financier[240] dans une société d'opérations immobilières », soit dans n'importe quel type d'entité avec laquelle elle fait affaire en conformité avec l'article 410[241]. Cette disposition a été modifiée en 1999 à la suite des propositions du Groupe de travail sur l'avenir du secteur des services financiers[242], de sorte que l'article 410(1)(c.1) leur permet de détenir une « société d'information », avec l'obtention préalable de l'accord du ministre. L'article 468(1) définit la société d'information comme une personne morale travaillant dans le secteur : a) de la conception, du développement et de la commercialisation de services de gestion de d'information ou b) de logiciel. En fait, les récentes modifications apportées en 1999 à la *Loi sur les banques*[243] lui permettent d'opérer une structure de société de portefeuille. En particulier, la loi l'autorise à détenir une institution financière autre qu'une banque à charte ou une autre entité qui offre d'autres services financiers – comme les services de cartes de crédit – si elle détient le contrôle *de facto*, ou une autre entité, auquel cas aucune exigence de contrôle n'est requise. Un service de certification pourrait être considéré comme une entité non financière, ce qui signifie que la banque pourra détenir sans contrainte une autorité

---

240 Selon l'article 10(1) de la *Loi sur les banques*, une banque possède un « intérêt de groupe financier » lorsqu'elle possède : *a*) plus de 10 pour cent des actions comportant un droit de vote, ou *b*) plus de 25 pour cent de l'avoir des actionnaires.

241 Selon l'article 100(1) de la *Loi constituant l'Agence de la consommation en matière financière du Canada et modifiant certaines lois relatives aux institutions financières*, L.C. 2001, c. 9, modifiant l'article 410(1)(c.1) de la *Loi sur les banques*, précitée, note 239, une banque peut, avec l'accord préalable du ministre « s'occuper, notamment en les concevant, les développant, les détenant, les gérant, les fabriquant ou les vendant, de systèmes de transmission de données, de sites d'information, de moyens de communication ou de plates-formes informatiques ou de portails d'information » utilisés dans les cas suivants : « (i) soit pour la fourniture d'information principalement de nature financière ou économique ; (ii) soit pour la fourniture d'information relative à l'activité commerciale des entités admissibles, au sens du paragraphe 464(1) ; (iii) soit à une fin réglementaire ou dans des circonstances réglementaires ». L'approche du projet de loi C-8 sur cette question s'éloigne du projet de loi C-67, sanctionné le 17 juin 1999 : *Loi modifiant* la Loi sur les banques*, la* Loi sur les liquidations et les restructurations *et d'autres lois relatives aux institutions financières et apportant des modifications corrélatives à certaines lois*, L.C. 1999, c. 28.

242 GROUPE DE TRAVAIL SUR L'AVENIR DU SECTEUR DES SERVICES FINANCIERS, *Changement, défis et possibilités*, Ottawa, Ministère des Finances, 1998, mieux connu sous le nom de « Rapport MacKay ».

243 L.R.C. 1991, c. 46, modifiée par la *Loi constituant l'Agence de la consommation en matière financière du Canada et modifiant certaines lois relatives aux institutions financières*, précitée, note 241.

de certification. Toutefois, rien n'empêche la banque d'acquérir, non seulement un contrôle *de facto*, mais un « intérêt de groupe financier »[244], lui autorisant le contrôle *de jure* sur l'entité détenue[245]. Aux États-Unis, l'Office of the Comptroller of the Currency (ci-après cité « OCC ») a accueilli la requête de la Zions First National Bank au sujet de l'établissement d'une filiale agissant en tant qu'autorité de certification pour la vérification de signatures électroniques et de dépositaire pour les certificats[246]. L'OCC a souligné l'importance, dès 1998, des autorités de certification dans le commerce électronique : « *The ability of banks to act as certificate authorities for digital signatures is expected to be vital to their role in the evolving electronic payments systems* »[247]. Elle a conclu que les services d'autorité de certification représentent une partie accessoire des activités bancaires. En particulier, elle note : « *The concept that the "business of banking" can evolve to reflect logical outgrowths from the special skills, expertise, and competencies of banks is not new* »[248]. C'est dans ce contexte que l'OCC a produit des lignes directrices en 1999[249].

---

244 Selon l'article 10(1) de la *Loi sur les banques*, précitée, note 239, une banque possède un « intérêt de groupe financier » lorsqu'elle possède : *a*) plus de 10 pour cent des actions comportant un droit de vote, ou *b*) plus de 25 pour cent de l'avoir des actionnaires.

245 L'article 3(1)(a) énonce que le contrôle est *de jure* lorsque les actions comportant un droit de vote détenues par une banque excèdent 50 pour cent. Toutefois, le paragraphe *d*) établit une présomption de contrôle de fait « quand elle-même et les entités qu'elle contrôle détiennent la propriété effective d'un nombre de titres de la première tel que, si elle-même et les entités contrôlées étaient une seule personne, elle contrôlerait l'entité en question ».

246 OCC, *Conditional Approval n° 267*, Washington (DC), 2 janvier 1998, p. 1, en ligne : [http://www.occ.treas.gov/netbank/ibi.htm]. L'approbation a été sujette à deux conditions. Le requérant devait fournir une description complète du système d'information proposé à l'OCC avant le début des opérations et également informer les vendeurs potentiels que le contrat était sujet à une supervision par l'OCC.

247 *Id.*, p. 16.

248 *Id.*, p. 13.

249 OCC, *OCC Bulletin 99-20 : Certification Authority Systems*, Washington (DC), 4 mai 1999, en ligne : [http://www.occ.treas.gov/netbank/ibi.htm] (ci-après cité « OCC Bulletin 99-20 »). Voir de plus les bulletins suivants relatifs à ces lignes directrices : OCC, *OCC Bulletin 98-38 : Technology Risk Management : PC Banking*, Washington (DC), 24 août 1998, en ligne : [http://www.occ.treas.gov/netbank/ebguide.htm], et OCC, *OCC Bulletin 98-3 : Technology Risk Management*, Washington (DC), 4 février 1998, en ligne : [http://www.occ.treas.gov/netbank/ebguide.htm] ; John L. DOUGLAS et Thomas R. CROCKER, « A Decision

Ce nouveau service fait partie, à nos yeux, du concept canadien d'opération bancaire[250].

Le droit des sociétés par actions énonce qu'une société mère ne sera pas responsable pour les actes de sa filiale, sous réserve que ceux-ci aient servi à masquer une fraude, un abus de droit ou une contravention à l'ordre public[251]. En droit bancaire, les succursales sont des entités distinctes, mais en pratique, une banque peut être tenue responsable pour les actes de sa succursale, en particulier pour les erreurs et les fraudes commises par ses dirigeants[252]. En fait, lorsqu'un dirigeant engage la responsabilité de la banque, le client doit poursuivre la succursale, mais dans les faits, lorsque le litige est important, le contentieux du siège social de la banque sera concerné. Les caisses populaires fonctionnent différemment, car le client doit poursuivre directement la caisse à moins qu'une faute ne puisse être reprochée à la fédération[253].

Deuxièmement, dans la quête de la qualification de la relation juridique entre la banque et l'autorité de certification, la théorie du

---

Letting Bank Subsidiaries Act as Certification Authorities for Digital Signature Verification Will Increase Bank Forays into Electronic Commerce », (6 février 1998) *Nat'l L.J.* B4 (col. 1).

250 Pour une discussion plus approfondie du concept d'opération bancaire, voir notamment au Canada : Marc LACOURSIÈRE, « La réglementation des banques virtuelles au Canada », (2004) 49 *R.D. McGill* 683, 690-698.

251 Au Québec : art. 317 C.c.Q. Cette disposition codifie le droit existant en la matière : GOUVERNEMENT DU QUÉBEC, *Commentaires du ministre de la Justice, le Code civil du Québec*, t. 2, Québec, Publications du Québec, 1993, p. 213. Au sujet de cette disposition, voir : Maurice MARTEL et Paul MARTEL, *La compagnie au Québec*, t. I, Montréal, Wilson & Lafleur, 1999, p. 1-62–1-74 ; Stéphane ROUSSEAU, « Immunité des actionnaires et levée du voile corporatif : perspectives de l'analyse économique du droit », (1999) 78 *R. du B. can.* 1. En common law : *1005633 Ontario Inc.* c. *Winchester Arms Ltd.*, [2000] O.J. (Quicklaw) nº 2404, par. 89 et 90 (S.C.) ; *Rafiki Properties Ltd.* c. *Integrated Housing Development Ltd.*, [1999] B.C.J. (Quicklaw) nº 243, par. 11 et 17 (S.C.) ; *Constitution Insurance Co. of Canada* c. *Kosmopoulos*, [1987] 1 R.C.S. 2, (1987) 34 D.L.R. (4th) 208 ; *Canada Life Assurance Co.* c. *Canadian Imperial Bank of Commerce*, (1974) 3 O.R. (2nd) 70, 84 et 85, 44 D.L.R. (3rd) 486 (C.A.), demande d'appel à la Cour suprême du Canada refusée : [1974] R.C.S. viii.

252 *Parmar* c. *Banque Royale du Canada*, [1992] R.R.A. 931 (C.A.) ; N. L'HEUREUX, É. FORTIN et M. LACOURSIÈRE, *op. cit.*, note 8, nº 1.150, p. 254-256.

253 *Supermarché Coulombe Inc.* c. *Fédération des caisses populaires Desjardins de Québec*, [1997] R.D.T. 635, J.E. 97-2 (C.A.).

mandat pourrait trouver une utilité dans l'hypothèse où le certificateur ne possède aucun lien corporatif avec la banque. En effet, il pourrait être allégué que la banque donne un mandat à une autorité de certification d'agir en son nom en tant que certificateur. Sur ce point, il est intéressant de noter que l'ancien article 46-3-308(2) de l'*Utah Digital Signature Act*[254], qui ne trouvait pas d'équivalent dans la *Loi concernant le cadre juridique des technologies de l'information*[255], prévoyait que :

> (a) a licensed certification authority is not liable *for any loss caused by a false or forged digital signature of a subscriber*, if, *with respect to the false or forged digital signature*, the certification authority complied with the requirements of this chapter ;
>
> (b) a licensed certification authority is not liable *for a misrepresentation in the certificate, or for error in issuing the certificate* in excess of the amount specified in the certificate as the recommended reliance limit. (nos non-italiques)

Une interprétation littérale de ce texte signifie que la responsabilité de l'autorité de certification est engagée lorsqu'elle ne respecte pas les dispositions de cette loi. Puisque ce problème pourrait se poser en droit québécois, peut-on affirmer que l'autorité de certification outrepasse son mandat ? L'article 2160 C.c.Q. dispose que le « mandant est tenu envers le tiers pour les actes accomplis par le mandataire *dans l'exécution et les limites du mandat*, sauf si, par la convention ou les usages, le mandataire est seul tenu. *Il est aussi tenu des actes qui excédaient les limites du mandat et qu'il a ratifiés* » (nos italiques). Ainsi, une banque, agissant en tant que mandante, ne serait pas responsable lorsque l'autorité de certification, soit la mandataire, excède les limites de son mandat, à moins d'avoir ratifié ces actes. L'intensité de cette obligation est moindre pour la banque dans l'hypothèse d'une relation contractuelle de mandat que lorsque la relation est corporative.

Troisièmement, une autorité de certification pourrait être considérée comme étant liée à la banque par un contrat d'entreprise ou de service, car d'une part, l'entrepreneur a le libre choix des moyens d'exécution du contrat et, d'autre part, il n'existe aucun lien de

---

254 Précitée, note 56.

255 Précitée, note 1.

subordination[256]. L'article 2098 C.c.Q. définit ce contrat comme étant « celui par lequel une personne, selon le cas l'entrepreneur ou le prestataire de services, s'engage envers une autre personne, le client, à réaliser un ouvrage matériel ou intellectuel ou à fournir un service moyennant un prix que le client s'oblige à lui payer ». En pratique, une autorité de certification offre des services principalement de nature intellectuelle, mais qui peuvent être accessoirement matériels.

La banque, considérée comme le donneur d'ouvrage, est tenue principalement à une obligation précontractuelle de renseignements[257] et, d'une manière générale, à une obligation de diligence[258]. En fait, cette obligation peut être assimilée à l'obligation de diligence prévue par le droit bancaire[259]. Cette troisième hypothèse impose donc moins de responsabilités à la banque que la forme corporative ou le mandat.

Un client ayant un lien de droit avec une autorité de certification de niveau inférieur conserve un droit d'action envers la banque – dans l'hypothèse d'une relation corporative ou contractuelle avec la banque – car l'intensité de l'obligation de la banque à cet égard repose principalement sur l'obligation d'agir avec prudence et diligence, tel que mentionné plus haut[260], de même qu'avec l'obligation de loyauté[261]. Or, le client de la banque n'a toutefois pas de lien direct avec une autorité de certification de niveau supérieur, mais il peut espérer obtenir gain de cause contre une banque qui ne respecte pas les ordonnances ou les directives de cette autorité, que la banque soit liée ou non à cette autorité de niveau supérieur. Sur ce point, il est intéressant de procéder par analogie avec la responsabilité de la banque pour le non-respect des règles des chambres de compensation interbancaires[262]. Lorsqu'une banque ne respecte

---

256 Art. 2099 C.c.Q.

257 *Banque de Montréal* c. *Bail Ltée*, [1992] 2 R.C.S. 554. Il en va de même pour le prestataire de services à l'égard de la banque : art. 2102 C.c.Q.

258 Art. 2100 C.c.Q.

259 N. L'HEUREUX, É. FORTIN et M. LACOURSIÈRE, *op. cit.*, note 8, première partie, titre IV, c. I (nº 1.146-1.168, p. 305-334).

260 Voir *supra*, notes 227, 258 et 259 et les textes correspondants.

261 Voir généralement : N. L'HEUREUX, É. FORTIN et M. LACOURSIÈRE, *op. cit.*, note 8, première partie, titre IV, c. II (nº 1.169-1.174, p. 337-349).

262 Les chambres de compensation interbancaires émettent des règles auxquelles les banques doivent se soumettre.

pas les règles de la chambre de compensation, elle peut être tenue responsable envers son client[263]. Cette question nécessite de qualifier la relation entre la banque et la chambre de compensation. Les règles des chambres de compensation prévoient que les relations entre les banques et ces dernières sont contractuelles et non fondées sur une relation de mandat, car les banques sont considérées comme des membres d'une chambre de compensation[264]. Il pourrait donc être allégué que cette relation se rapproche du contrat de service, puisque la chambre offre le service de compensation à la banque. La jurisprudence et la doctrine édictent que les règles formulées par les réseaux interbancaires font partie implicite du contrat bancaire conclu entre le client et la banque. À cet égard, dans la décision *Stanley Works of Canada Ltd.* c. *Banque Canadienne Nationale*[265], la Cour d'appel a jugé qu'une banque tirée est responsable envers le tireur d'un chèque si elle ne respecte pas les règles de la chambre de compensation, car elle doit protéger les intérêts de son client[266]. Celui-ci peut donc se fonder sur la négligence de la chambre de compensation pour tenir la banque responsable envers lui-même.

Toujours en ce qui concerne l'obligation de diligence, considérons, par analogie, le cas d'une banque qui n'exécute pas les ordres de son client, comme à titre d'exemple lors d'un transfert de fonds : celle-ci est responsable envers son client pour ne pas avoir agi avec

---

263 *Stanley Works of Canada Ltd.* c. *Banque Canadienne Nationale*, [1982] R.L. 433, (1982) 20 B.L.R. 282 (C.A.) (ci-après avec renvois à la R.L.) ; *Process Piping Specialities Inc.* c. *Banque Canadienne Nationale du Canada*, [1986] R.J.Q. 2429 (C.S.).

264 *British Eagle International Airlines Ltd.* c. *Compagnie Air France*, [1975] 2 All E.R. 390, 405, [1975] 1 W.L.R. 758 (H.L.) ; Ross CRANSTON, *Principles of Banking Law*, Oxford, Clarendon Press, 1997, p. 310.

265 *Stanley Works of Canada Ltd.* c. *Banque Canadienne Nationale*, précité, note 263.

266 *Id.*, 438. Plus précisément, la banque tirée avait débité le compte de son client après le délai de 48 heures – maintenant 24 heures – dont elle disposait pour ce faire et, par conséquent, le chèque a été retourné pour fonds insuffisants, ce qui a créé un préjudice au client. Ce dernier a allégué avec succès que la banque avait été négligente en n'agissant pas dans le délai requis. La Cour a ajouté que la banque ne pouvait se libérer de ce devoir et devait protéger les intérêts de son client. Voir : Bradley CRAWFORD, *Crawford and Falconbridge – Banking and Bills of Exchange*, Aurora, Canada Law Book, 1986, n° 3203(a), p. 746 ; N. L'HEUREUX, É. FORTIN et M. LACOURSIÈRE, *op. cit.*, note 8, n° 1.23, p. 89-90 ; Jérôme CHOQUETTE, « Chronique de législation et de jurisprudence », (1982) 60 *R. du B. can.* 746.

la diligence nécessaire en de telles circonstances[267]. D'ailleurs, les banques sont déjà familiarisées avec les systèmes de sécurité utilisés à des fins précises, notamment pour les cartes de débit[268], et une banque qui ne respecte pas cette obligation engage sa responsabilité[269]. Pour ce qui est de l'obligation de loyauté, la raison d'être de celle-ci repose sur un contrat fondé sur la confiance[270], ce critère étant le but essentiel recherché – la confiance en la sécurité – par les parties qui utilisent les services d'une autorité de certification.

Quatrièmement, il peut n'exister aucun lien juridique entre la banque et l'autorité de certification. Alors que les trois premières situations s'appliquent principalement à des autorités de certification de niveau de base, il est possible que la banque ne soit pas liée de manière corporative ou contractuelle à une autorité de certification supérieure. En principe, il n'existe aucun lien de droit entre celle-ci et la banque, puisque la banque a un lien avec l'autorité subalterne et non avec le niveau supérieur. Or, nous avons mentionné plus haut qu'il existe des situations d'autosupervision et d'autocertification pyramidale ainsi que des hiérarchies trompeuses. Ces cas particuliers suggèrent qu'il pourrait exister un lien de droit, selon les formes décrites précédemment, avec les conséquences qui en découlent.

Dans l'hypothèse où il n'existe aucun lien de droit entre la banque et l'autorité de certification de niveau supérieur, un client pourrait tenir la banque responsable non seulement en vertu des principes de la responsabilité civile extracontractuelle, mais également selon la relation contractuelle. En effet, bien qu'il n'existe aucun lien de droit entre la banque et l'autorité, la banque demeure la mandataire de son client lorsqu'elle lui offre un service autre que la gestion

---

267 N. L'HEUREUX, É. FORTIN et M. LACOURSIÈRE, *op. cit.*, note 8, nº 1.152, p. 313-315.

268 Le réseau interbancaire Interac garantit une haute sécurité pour ces types de paiements. Voir le portail d'Interac : [http://www.interac.ca].

269 Dans la très célèbre décision *Evra Corp.* c. *Swiss Bank Co.*, 673 F.2d 951 (7th Cir. 1982), une banque a été tenue responsable pour les dommages directs causés par le manque de papier dans son télécopieur, ce qui l'a empêchée de recevoir un ordre de paiement.

270 N. L'HEUREUX, É. FORTIN et M. LACOURSIÈRE, *op. cit.*, note 8, nº 1.170(b), p. 339.

d'un compte de banque[271] comme, à titre d'exemple, le traitement d'un chèque. La théorie de la Cour d'appel développée dans la décision *Stanley Works of Canada Ltd.* c. *Banque Canadienne Nationale*[272] pourrait trouver application en l'espèce, surtout, si l'on considère une chambre de compensation comme une autorité de certification de niveau supérieure.

3. Les clauses exonératoires

En droit québécois, les articles 1470 C.c.Q. et suivants permettent à une personne de s'exonérer de sa responsabilité. Ce concept, interprété de manière restrictive[273], s'applique en droit bancaire, que ce soit pour les transactions commerciales ou de consommation[274]. Dans ce dernier cas, les banques utilisent couramment les clauses exonératoires dans les contrats de cartes de débit, de cartes de crédit, de prêts bancaires et de contrats bancaires en ligne[275], notamment. En fait, les banques utilisent les clauses exonératoires depuis environ un siècle dans les accords de vérification[276]. Au fil du temps, les juges ont balisé les conditions de validité de ces accords, et les banques les ont raffinés pour atteindre ce qui peut être qualifié de point d'équilibre[277].

L'article 1474 C.c.Q. apporte un tempérament à la validité des clauses exonératoires, car il empêche quiconque de s'exonérer en

---

271 Dans ce cas, la relation est de débiteur-créancier, car le dépôt bancaire équivaut à un prêt : *Foley* c. *Hill*, 2 H.L.C. 28, 9 E.R. 1002 (1848).

272 *Stanley Works of Canada Ltd.* c. *Banque Canadienne Nationale*, précité, note 263.

273 Au Québec : *Meany* c. *Caisse populaire Ste-Geneviève de Pierrefonds*, [1991] R.R.A. 813 (C.Q.) ; art. 1474 C.c.Q.

274 À titre d'exemple, voir au Québec : *Loi sur la protection du consommateur*, L.R.Q., c. P-40.1, art. 10 ; *Lévesque* c. *Concept santé Nautilus*, [1996] R.R.A. 733 (C.S.) ; *Gosselin* c. *Services de voyages Yves Bordeleau Inc.*, [1990] R.J.Q. 1454 (C.Q.) ; Nicole L'HEUREUX, *Droit de la consommation*, Cowansville, Éditions Yvon Blais, 2000, nº 42, p. 54-56. Voir également en Ontario : *Loi sur la protection du consommateur*, L.R.O. 1990, c. C.31, art. 33.

275 Les exonérations sont particulièrement onéreuses dans ces contrats.

276 *Columbia Graphophone Co.* c. *Union Bank of Canada*, (1916) 38 O.L.R. 326, (1917) 34 D.L.R. 743 (H.C. Ont.).

277 *Arrow Transfer Company Ltd.* c. *Banque Royale du Canada*, [1972] R.C.S. 845 ; *Société hôtelière Canadien Pacifique Ltée* c. *Banque de Montréal*, [1987] 1 R.C.S. 711.

cas de faute lourde, celle-ci étant habituellement associée à la négligence grossière ou à la fraude. À titre d'exemple, dans la décision *Banque de Nouvelle-Écosse* c. *Angelica-Whitewear Ltd.*, la Cour suprême du Canada a jugé qu'une clause d'exonération de responsabilité contenue dans une entente entre la banque et son client « ne relèverait pas la [b]anque de l'obligation d'honorer la traite si elle avait connaissance de la fraude de la bénéficiaire du crédit »[278]. Cette vision a été reprise dans la décision *Les Entreprises Wyknott International Inc.* c. *Banca Commerciale Italiana of Canada*[279], où la Cour du Québec a déclaré qu'une banque ne pouvait limiter sa responsabilité dans le cas d'une fraude d'une traite régie par les *Règles uniformes pour l'encaissement de papier commercial*[280].

Les clauses exonératoires des sites bancaires en ligne sont particulièrement contraignantes à l'égard des clients[281]. Il est possible de croire que cette tendance ne diminuerait pas dans l'hypothèse d'une relation juridique entre une banque et une autorité de certification. À titre d'exemple, les autorités de certification Verisign et

---

278 *Banque de Nouvelle-Écosse* c. *Angelica-Whitewear Ltd.*, [1987] 1 R.C.S. 59, 108 et 109, (1987) 36 D.L.R. (4th) 161. Voir de plus : *Morguard Trust Co.* c. *Royal Bank of Canada*, (1988) 60 Alta. L.R. (2nd) 99, 121, [1988] 5 W.W.R. 415 (Q.B.), confirmé par (1989) 71 Alta. L.R. (2nd) 85, 104 A.R. 22 (C.A.). Sur la question de la fraude, voir également les décisions antérieures à l'affaire *Angelica-Whitewear* : *Stewart Estate* c. *Royal Bank*, [1930] R.C.S. 544, 549, [1930] 4 D.L.R. 694 ; *Levasseur* c. *Banque de Montréal*, [1978] C.S. 1157, 1159.

279 *Les Entreprises Wyknott International Inc.* c. *Banca Commerciale Italiana of Canada*, [1998] R.R.A. 922, REJB 1998-05958 (C.Q.).

280 CCI, *Règles uniformes pour l'encaissement de papier commercial*, Paris, Publication CCI, 1967, Pub. n° 254. Voir plus récemment : *Règles uniformes relatives aux encaissements documentaires*, Paris, Publications CCI, 1995, Pub. n° 522. En l'espèce, la Cour a jugé que la Banca Commerciale n'avait pas agi avec prudence et diligence et qu'elle avait commis une négligence grossière puisqu'elle ne s'était pas informée si la traite avait été délivrée à temps.

281 À titre d'exemple, le site de la Banque Nationale du Canada prévoit qu'elle-même, « ses filiales et ses sociétés affiliées dégagent leur responsabilité de tous dommages que vous pourriez subir découlant de l'échange de renseignements avec elles » : BANQUE NATIONALE DU CANADA, *Avis important à tous les utilisateurs du site Internet de la Banque Nationale du Canada*, Montréal, 1998, en ligne : [http://www.bnc.ca/index.html]. À la Banque de Montréal, la clause de non-responsabilité est similaire : « La Banque de Montréal, et ses filiales et sociétés affiliées, ne sont pas responsables de quelque manière que ce soit, des dommages directs, indirects, spéciaux ou consécutifs, ou pour quelque raison que ce soit, découlant de l'utilisation du présent site Web » : BANQUE DE MONTRÉAL, *Avis importants à tous les utilisateurs de ce site web*, Montréal, 2000, en ligne : [http://www.bmo.com/francais/legal/index.html].

Thawte commencent leurs « engagements de confiance » (« *Relying Party Agreement* ») en précisant que l'usager doit lire cet engagement et y acquiescer avant d'accorder sa confiance à un certificat issu de ces autorités[282]. L'autorité de certification Entrust précise que l'accès à un site sécurisé par elle-même constitue un contrat qui oblige l'usager à se soumettre à cet engagement de confiance[283]. Ces accords comportent notamment une limitation de responsabilité considérable :

> *You agree that your use of Verisign's (Thawte's) service(s) is solely at your own risk* [...] *Verisign (Thawte) does not make any warranty, term, condition or representation as to the results that may be obtained from the use of the service or to the* accuracy or reliability of any information obtained through the service[284] (nos non-italiques).

> The entire risk of the use *of any Entrust SSL Web Server Certificates or any services provided in respect Entrust* [sic] *SSL Web Server Certificates* or the validation of digital signatures shall be borne solely by you[285] (nos non-italiques).

Il est également important de souligner que ces engagements de confiance sont difficilement accessibles. L'internaute doit cliquer sur l'icône de sécurité du site auquel il accède et ensuite consulter la « Déclaration de l'émetteur » en cliquant sur une seconde icône. De plus, la « Déclaration de l'émetteur » de l'autorité de certification Entrust renvoie à une page Web inexistante et l'adresse actuelle de l'engagement de confiance n'est accessible qu'en cliquant sur une troisième icône « Plus d'info ». De plus, ces engagements de confiance ne sont pas disponibles en français.

*
* *

À ce jour, la sécurité des transactions bancaires en réseau ouvert peut être assurée par plusieurs moyens techniques, notam-

---

282 VERISIGN, « Relying Party Agreement », en ligne : [https://www.verisign.com/repository/rpa.html] ; THAWTE, « Relying Party Agreement », en ligne : [http://www.thawte.com/ssl-digital-certificates/free-guides-whitepapers/pdf/cpsrelyingparty.pdf].

283 ENTRUST, « SSL Web Server Certificate Relying Party Agreement », en ligne : [http://www.entrust.net/relying/pdf/webrelying010103.pdf].

284 VERISIGN, *loc. cit.*, note 282, nº 10 ; THAWTE, *loc. cit.*, note 282, 4.

285 ENTRUST, *loc. cit.*, note 283, 3.

ment par le système de cryptographie à clé publique. L'intérêt de ce système tient au fait qu'il nécessite l'intervention d'une tierce personne qui doit certifier l'intégrité de l'identification du transmetteur et/ou du récepteur, ainsi que l'intégrité des données lors de leur transmission. Cette idée n'est pas nouvelle, certes, mais dans le contexte d'Internet, ce tiers certificateur constitue un joueur clé. En fait, le développement d'un environnement bancaire sécuritaire ne peut négliger l'utilisation de ce système de sécurité. L'utilisation de la cryptographie asymétrique par les réseaux de communication interbancaires CHIPS[286] et SWIFT dans des projets récents témoigne de cette nécessité[287].

Une infrastructure hiérarchique de cryptographie à clé publique permet également de sécuriser les opérations bancaires en ligne. Il existe plusieurs types d'infrastructures de cryptographie à clé publique. Dans un monde idéal, une structure de type pyramidale qui consiste en une superposition de plusieurs niveaux verticaux serait souhaitable. Au niveau inférieur, une autorité de certification subalterne établit un contact directement avec les cocontractants. Ceci peut être le cas, notamment, d'un notaire qui émet une signature électronique ainsi qu'un certificat à une personne qui désire transmettre une information sensible par l'entremise d'Internet. Au niveau intermédiaire, une autorité de certification régionale – provinciale ou nationale – supervise l'autorité de certification subalterne. À titre d'exemple, l'ACP avait un projet en ce sens[288]. Au niveau supérieur, une autorité de certification internationale, par exemple, peut superviser l'autorité précédente. Il va de soi que le nombre de niveaux de confiance peut varier. Plus une hiérarchie de certification comporte de niveaux, plus l'internaute doit effectuer de vérifications, ce qui est paradoxal, puisqu'une hiérarchie élaborée suppose plus de sécurité[289].

---

286 CHIPS, « CHIPS Takes Next Step Towards a Complete B2B Solution », février 2001, en ligne : [http://www.chips.org/news.htm] ; CHIPS, *UPIC Implementation Manual*, version 1.1, août 2002, en ligne : [http://www.chips.org/infofiles/CHIPS_UPIC_Implementation_guide.pdf].

287 SWIFT, « e-paymentsPlus Services Overview », mars 2002, en ligne : [http://www.swift.com/temp/41760/7552/1_e-paymentsPlus_R1_SO_v1.2.pdf].

288 ACP, « CPA PKI Business Strategy », Ottawa, 16 février 2000, en ligne : [http://www.cdnpay.ca/fre/pub/PKI310.pdf] ; ACP, « L'ACP cesse son initiative d'ICP », Ottawa, 2003, en ligne : [http://www.cdnpay.ca/news/pki_fr.asp].

289 A.M. FROOMKIN, *loc. cit.*, note 13, 56.

En pratique, cependant, le développement des systèmes de cryptographie à clé publique repose sur une fondation d'argile. Ces systèmes se limitent habituellement à un seul niveau, omettant l'implantation d'un processus de supervision par l'entremise d'une infrastructure hiérarchique. Cette situation semble paradoxale : le droit canadien permet non seulement qu'un seul tiers certificateur sécurise les transactions bancaires en ligne – notamment par l'émission et la vérification d'une signature électronique –, mais également que ce tiers certificateur soit exploité et même contrôlé par une banque. L'impact est important pour l'usager. Bien que ce dernier ne puisse saisir toutes les subtilités des lacunes dans le système de sécurité de sa banque, il en comprendra les conséquences dans l'éventualité d'une fraude : en effet, l'absence d'indépendance juridique du tiers certificateur affecte la qualité de la sécurité.

Pour contourner cette situation, il s'agit de respecter deux conditions fondamentales. D'abord, un tiers certificateur doit être indépendant pour acquérir la reconnaissance et la notoriété. Ensuite, il est nécessaire de superviser les activités de cette autorité de certification par l'entremise d'une infrastructure hiérarchique à paliers multiples, tel qu'expliqué précédemment. Or, en ce domaine, les premières tentatives s'avèrent infructueuses pour le moment. En février 2000, l'ACP a proposé de devenir une autorité de certification principale – de niveau supérieur –, mais elle a récemment suspendu ce projet[290]. L'ACP a justifié sa décision par le fait que « les projections du marché pour les applications de paiement par l'ACP ne justifient pas d'aller de l'avant avec la mise en œuvre ». Elle laisse toutefois porte ouverte à la reprise de ce projet, si l'évolution du marché canadien le nécessite[291]. L'échec de ce projet démontre la difficulté d'implantation d'une telle infrastructure de cryptographie à clé publique entièrement sécuritaire. Ceci confirme notre première hypothèse quant au fait que les autorités de certification opérées par les banques n'offrent pas le degré d'indépendance requis, et notre deuxième hypothèse, laquelle sous-entend qu'une infrastructure hiérarchique d'autorités de certification doit être mise en place dans le secteur bancaire canadien afin de sécuriser les opérations bancaires.

---

290 ACP, *loc. cit.*, note 288.

291 *Id.*

Les derniers développements en matière de certification et de sécurité des transactions en ligne concernent le niveau de chiffrement lié au protocole SSL. Les autorités de certification sont passées d'un chiffrement de 128 bits à un chiffrement de 1024 ou 2048 bits pour leurs signatures et certificats[292]. De plus, un nouveau protocole – *Server Gated Cryptography* – vise à accroître l'efficacité du SSL pour les navigateurs Web et les systèmes d'exploitation, car les versions antérieures de ces derniers ne supportent pas de chiffrement de haute performance[293]. Ces avancées technologiques touchent uniquement l'aspect informatique de la sécurité des transactions, mais ne modifient aucunement l'état actuel des infrastructures de certification existante.

Le secteur bancaire canadien n'a pas su, à ce jour, favoriser le développement d'un environnement juridique sécuritaire pour les consommateurs qui effectuent des opérations bancaires en ligne. Au Canada, seule la *Loi concernant le cadre juridique des technologies de l'information*[294] réglemente partiellement cette question, alors que les lois des autres provinces canadiennes sont silencieuses à cet égard. La *Loi uniforme sur le commerce électronique*[295], loi modèle issue de la Conférence, ne s'inspire que de la *Loi type de la CNUDCI sur le commerce électronique* et ne tient pas compte de la nouvelle *Loi type de la CNUDCI sur les signatures électroniques* qui complète cette dernière et aborde plus en détail la certification. Enfin, la *Loi sur la protection du consommateur*[296] est également muette au sujet des transactions en ligne, contrairement à d'autres lois canadiennes[297]. Ceci confirme notre dernière hypothèse, qui avance que les provinces canadiennes doivent tendre vers une certaine forme d'harmonisation en matière de sécurité des opérations bancaires par Internet pour assurer une meilleure protection des usagers.

---

292 VERISIGN, « Roots Certificates », en ligne : [https://www.verisign.com/repository/root.html].

293 VERISIGN, « Comment offrir le cryptage SSL le plus fiable du marché », Mountain View, Verisign, 2004, 2, en ligne : [http://www.verisign.fr/static/030138.pdf].

294 Précitée, note 1.

295 Précitée, note 39.

296 L.R.Q., c. P-40.1.

297 *Supra*, note 42.